



Acronis Backup für Windows Server

Version 11.5 Update 3

Benutzeranleitung

Urheberrechtserklärung

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,275,139; 7,281,104;7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; sowie schwebende Patentanmeldungen.

Inhaltsverzeichnis

1 Einführung in Acronis Backup

1.1 Die Neuerungen von Update 3

Änderung des Produktnamens

- Acronis Backup & Recovery 11.5 wurde zu Acronis Backup umbenannt.

Lizenzierung

- Die Universal Restore-Funktion ist in allen Acronis Backup-Lizenzen enthalten. Die Lizenz für das Universal Restore Add-on wurde entsprechend verworfen.

Cloud Backup

- Der Acronis Backup & Recovery Online Service wurde zu Acronis Cloud Backup umbenannt.
- Die Cloud Backup-Abonnements für Server und für virtuelle Maschinen wurden verworfen. Benutzer können diese Abonnements als bzw. zu Abonnements für mehrere Systeme (S. 286) erneuern.

Betriebssystemunterstützung

- Unterstützung für Windows MultiPoint Server 2012 und Windows Storage Server 2012 R2.

1.2 Die Neuerungen von Update 2

- Unterstützung für 'Abonnements für mehrere Systeme' für Acronis Backup & Recovery Online (S. 286).
- Unterstützung von WinPE 5.0.

1.3 Die Neuerungen von Update 1

Mit Build 37975 hinzugekommene Verbesserungen

- Basis-Unterstützung für Windows 8.1 und Windows Server 2012 R2.
- Installation von Acronis Backup & Recovery 11.5 im Testmodus ohne Lizenzschlüssel.
- Upgrade von einem Standalone-Produkt zur Advanced-Plattform, ohne dass die Software neu installiert werden muss.

Basis-Unterstützung für Windows 8 und Windows Server 2012 (S. 35)

- Installieren Sie Acronis Backup & Recovery 11.5 auf bzw. unter Windows 8 und dem Windows Server 2012.
- Booten Sie eine Maschine mit einem auf WinPE 4 basierenden Boot-Medium.
- Verwenden Sie ein bootfähiges Medium auf einer Maschine, auf der UEFI Secure Boot aktiviert ist.
- Führen Sie Backup- und Recovery-Aktionen (ohne Größenanpassung) mit Volumes durch, die das ReFS-Dateisystem verwenden oder beliebige Daten enthalten.
- Sichern Sie Speicherplätze (Storage Spaces) per Backup und stellen Sie diese am ursprünglichen Ort, zu anderen Speicherplätzen oder als gewöhnliche Laufwerke wieder her.
- Führen Sie Backup- und Recovery-Aktionen (auf Laufwerksebene) mit Volumes durch, auf denen die Datendeduplizierungsfunktion aktiviert ist.

Andere(s)

- Deaktivieren Sie die Backup-Katalogisierung (S. 87) vollständig.
- Speichern Sie einen Desaster-Recovery-Plan (S. 95) in einem lokalen Ordner oder Netzwerkordner (zusätzlich zum Versenden per E-Mail).
- Aktivieren Sie VSS-Voll-Backups (S. 109), um die Protokolle von VSS-kompatiblen Anwendungen nach einem Laufwerk-Backup abschneiden zu können.
- Booten Sie eine UEFI-Maschine mit einem auf 64-Bit WinPE basierenden (S. 195) Boot-Medium.
- Fügen Sie die Variable **%description%** (entspricht der in den Systemeigenschaften einer Windows-Maschine angezeigten Beschreibung) dem Betreff für die E-Mail-Benachrichtigung (S. 96) hinzu.

1.4 Die Neuerungen in Acronis Backup & Recovery 11.5

Nachfolgend finden Sie eine Zusammenfassung der neuen Produktfunktionen und Verbesserungen.

Unterstützung für zahlreiche Storage-Typen

Acronis Online Backup Storage

- Backups zum Acronis Online Backup Storage replizieren oder verschieben (S. 86).
- Die Backup-Schema 'Großvater-Vater-Sohn' und 'Türme von Hanoi' stehen jetzt auch bei Backups zum Acronis Online Backup Storage zur Verfügung.

Bootfähiges Medium

- Neue Linux-Kernel-Version (3.4.5) bei Linux-basierten bootfähigen Medien. Der neue Kernel bringt eine bessere Hardware-Unterstützung mit sich.

Benutzeroberfläche

- Unterstützung für eine Bildschirmauflösung von 800x600.

1.5 Acronis Backup-Komponenten

Dieser Abschnitt enthält eine Liste der Acronis Backup-Komponenten mit einer kurzen Beschreibung ihrer Funktionalität.

Komponenten für eine verwaltete Maschine (Agenten)

Dies sind Anwendungen zur Durchführung von Backups, Wiederherstellungen und anderen Aktionen auf Maschinen, die mit Acronis Backup verwaltet werden. Die Agenten benötigen je eine Lizenz zur Durchführung von Aktionen mit einer verwalteten Maschine.

Konsole

Die Konsole stellt eine grafische Benutzeroberfläche für die Agenten bereit. Zur Verwendung der Konsole wird keine Lizenz benötigt. Die Konsole wird zusammen mit dem Agenten installiert und kann von diesem nicht getrennt werden.

Bootable Media Builder

Mit dem Bootable Media Builder können Sie bootfähige Medien erstellen, damit Sie die Agenten und andere Notfallwerkzeuge in einer autonomen Notfallversion verwenden können. Der Bootable Media Builder wird zusammen mit dem Agenten installiert.

1.5.1 Agent für Windows

Dieser Agent ermöglicht unter Windows, Ihre Daten auf Laufwerk- und Datei-Ebene zu schützen.

Laufwerk-Backup

Der Schutz auf Laufwerksebene basiert auf Sicherung des gesamten Dateisystems eines Laufwerks bzw. Volumes, einschließlich aller zum Booten des Betriebssystems notwendigen Informationen; oder – beim Sektor-für-Sektor-Ansatz – auf Sicherung aller Laufwerkssektoren (raw-Modus). Ein Backup, welches die Kopie eines Laufwerks oder Volumes in gepackter Form enthält, wird auch Laufwerk-Backup (Disk-Backup, Partition-Backup, Volume-Backup) oder Laufwerk-Image (Partition-Image, Volume-Image) genannt. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Datei-Backup

Der Schutz der Daten auf Datei-Ebene basiert auf der Sicherung von Dateien und Ordnern, die sich auf der Maschine, auf der der Agent installiert ist oder auf einem freigegebenen Netzlaufwerk befinden. Dateien können an ihren ursprünglichen oder einen anderen Speicherort wiederhergestellt werden. Es ist möglich, alle gesicherten Dateien und Verzeichnisse wiederherzustellen. Sie können aber auch auswählen, welche Dateien und Verzeichnisse wiederhergestellt werden sollen.

Andere Aktionen

Konvertierung zu einer virtuellen Maschine

Der Agent für Windows führt die Konvertierung durch, indem er ein Laufwerk-Backup zu einer neuen virtuellen Maschine folgenden Typs wiederherstellt (wahlweise): VMware Workstation, Microsoft Virtual PC, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM (Kernel-based Virtual Machine). Die Dateien der vollständig konfigurierten und einsatzbereiten Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine zukünftige Verwendung vorbereiten.

Wiederherstellung auf abweichende Hardware

Sie können die Funktion zur Wiederherstellung auf abweichender Hardware auf derjenigen Maschine verwenden, auf welcher der Agent installiert ist. Außerdem können Sie bootfähige Medien mit dieser Funktion erstellen. Acronis Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind (beispielsweise Speicher-Controller, Mainboard oder Chipsatz).

Laufwerksverwaltung

Agent für Windows enthält Acronis Disk Director Lite - ein nützliches Werkzeug zur Laufwerksverwaltung. Aktionen zur Laufwerksverwaltung, wie das Klonen und Konvertieren von Laufwerken, das Erstellen, Formatieren und Löschen von Volumes; das Ändern des Partitionierungsschemas eines Laufwerks zwischen MBR und GPT oder das Ändern einer Laufwerksbezeichnung können sowohl im Betriebssystem als auch durch Nutzung eines bootfähigen Mediums durchgeführt werden.

1.5.2 Management Konsole

Acronis Backup Management Console ist ein administratives Werkzeug für den lokalen Zugriff auf den Acronis Backup Agent. Eine Remote-Verbindung mit dem Agenten ist nicht möglich.

1.5.3 Bootable Media Builder

Der Acronis Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung bootfähiger Medien (S. 296). Der auf Windows installierte Media Builder kann bootfähige Medien schaffen, die entweder auf Windows Preinstallation Environment (WinPE) oder einem Linux-Kernel basieren.

1.6 Über die Verwendung des Produktes im Testmodus

Bevor Sie eine Lizenz von Acronis Backup kaufen, möchten Sie die Software möglicherweise testen. Dies kann ohne einen Lizenzschlüssel getan werden.

Führen Sie zur Installation des Produktes im Testmodus das Setup-Programm lokal aus oder verwenden Sie die Möglichkeit zur Remote-Installation. Eine unbeaufsichtigte Installation oder andere Installationsvarianten werden nicht unterstützt.

Beschränkungen des Testmodus

Wenn Acronis Backup im Testmodus installiert wurde, hat es folgende Beschränkungen:

- Die Funktion 'Universal Restore' ist deaktiviert.

Zusätzliche Beschränkungen für bootfähige Medien:

- Die Funktion zur Laufwerksverwaltung ist nicht verfügbar. Sie können alles innerhalb der Benutzeroberfläche testen, aber die Option zur Umsetzung ausstehender Aktionen ist nicht verfügbar.
- Die Recovery-Funktion ist verfügbar, jedoch keine Backup-Funktion. Installieren Sie die Software im Betriebssystem, um auch die Backup-Funktion testen zu können.

Upgrade auf die Vollversion

Nach Ablauf des Testzeitraums wird auf der Benutzeroberfläche des Produkts eine Meldung angezeigt, die Sie dazu auffordert, einen Lizenzschlüssel zu spezifizieren oder zu erwerben.

Um einen Lizenzschlüssel spezifizieren zu können, müssen Sie auf **Hilfe** –> **Lizenz wechseln** (S. 263) klicken. Es ist nicht möglich, den Schlüssel durch Ausführung des Setup-Programms zu spezifizieren.

Falls Sie ein Test- oder Kaufabonnement für den Cloud Backup Service (S. 271) aktiviert haben, steht Ihnen die Cloud Backup-Funktion bis zum Ende des Abonnementzeitraums zur Verfügung – unabhängig davon, ob Sie einen Lizenzschlüssel spezifizieren.

1.7 Unterstützte Dateisysteme

Acronis Backup kann Backups und Wiederherstellungen der folgenden Dateisysteme mit den angegebenen Einschränkungen ausführen:

- FAT16/32
- NTFS
- ReFS – Volume-Recovery ohne die Möglichkeit, die Größe des Volumes zu ändern. Wird nur in Windows Server 2012/2012 R2 (S. 35) unterstützt.
- Ext2/Ext3/Ext4
- ReiserFS3 – aus Laufwerk-Backups, die sich auf dem Acronis Backup Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden

- ReiserFS4 – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Laufwerk-Backups, die sich auf dem Storage Node in Acronis Backup befinden, können keine einzelnen Dateien wiederhergestellt werden
- XFS – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Disk-Backups, die sich auf dem Storage Node in Acronis Backup befinden, können keine einzelnen Dateien wiederhergestellt werden
- JFS – aus Laufwerk-Backups, die sich auf dem Acronis Backup Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden
- Linux SWAP

Acronis Backup kann unter Verwendung eines Sektor-für-Sektor-Ansatzes Backups und Wiederherstellungen bei beschädigten oder nicht unterstützten Dateisystemen ausführen.

1.8 Technischer Support

Maintenance- und Support-Programm

Wenn Sie Unterstützung für Ihr Acronis-Produkt benötigen, besuchen Sie http://www.acronis.de/support

Produkt-Updates

Sie können für all Ihre registrierten Acronis-Software-Produkte jederzeit Updates von unserer Website herunterladen, nachdem Sie sich unter **Mein Konto** (http://www.acronis.de/my) eingeloggt und Ihr Programm registriert haben. Weitere Informationen auch in den (englischsprachigen) Artikel unter **Registering Acronis Products at the Website** (http://kb.acronis.com/content/4834) und **Acronis Website User Guide** (http://kb.acronis.com/content/8128).

2 Erste Schritte



Schritt 1: Installation

Diese kurze Installationsanleitung ermöglicht Ihnen, schnell mit der Verwendung des Programms zu beginnen. Zu einer kompletten Beschreibung der Installationsmethoden und Prozeduren siehe die 'Installationsanleitung'.

Stellen Sie vor der Installation Folgendes sicher:

- Ihre Hardware erfüllt die Systemanforderungen.
- Sie haben für das Produkt Ihrer Wahl die entsprechenden Lizenzschlüssel.
- Sie haben das Setup-Programm. Sie können es von der Acronis-Website herunterladen.

So installieren Sie Acronis Backup

Führen Sie das Setup-Programm von Acronis Backup aus und folgen Sie den angezeigten Anweisungen.



Schritt 2: Ausführung

Starten Sie Acronis Backup, indem Sie den Eintrag **Acronis Backup** aus dem **Start**-Menü wählen.

Informationen zu den Elementen der grafischen Benutzeroberfläche finden Sie unter 'Management Konsole verwenden (S. 15)'.



Schritt 3: Bootfähige Medien

Erstellen Sie ein bootfähiges Medium, damit Sie ein (nicht mehr startfähiges) Betriebssystem wiederherstellen oder auf fabrikneuer Hardware bereitstellen können.

1. Wählen Sie **Werkzeuge –>** **Bootfähiges Medium erstellen** aus dem Menü.
2. Klicken Sie in der Willkommenseite auf **Weiter**. Klicken Sie solange auf **Weiter**, bis die Liste der Komponenten erscheint.
3. Fahren Sie wie im Abschnitt 'Linux-basiertes bootfähiges Medium (S. 190)' beschrieben fort.



Schritt 4: Backup



Backup jetzt (S. 38)

Klicken Sie auf **Backup jetzt**, um ein einmaliges Backup mit wenigen einfachen Schritten durchzuführen. Der Backup-Prozess wird unmittelbar ausgeführt, sobald Sie alle benötigten Schritte durchgeführt haben.

So speichern Sie Ihre Maschine in eine Datei:

Klicken Sie unter **Backup-Ziel** auf **Speicherort** und wählen Sie dann, wo das Backup gespeichert werden soll. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen. Klicken Sie im unteren Fensterbereich auf **OK**, um das Backup zu starten.

Tipp: Durch Verwendung eines bootfähigen Mediums können Sie Offline-Backups ('kalte' Backups) auf dieselbe Art erstellen wie im Betriebssystem.

 **Backup-Plan erstellen** (S. 38)

Erstellen Sie einen Backup-Plan, falls Sie eine langfristige Backup-Strategie benötigen, die Backup-Schema sowie Planungen und Bedingungen einschließt, um Backups zeitabhängig zu löschen oder sie zu anderen Orten zu verschieben.



Schritte 5: Recovery

 **Recovery** (S. 112)

Sie müssen für eine Wiederherstellung die im Backup gesicherten Daten wählen – sowie den Zielort, an dem die Daten wiederhergestellt werden sollen. Als Ergebnis dieser Aktion wird ein Recovery-Task erstellt.

Die Wiederherstellung eines Laufwerks bzw. Volumes über ein Volume, welches durch das Betriebssystem gesperrt ist, erfordert einen Neustart. Nach dem Abschluss der Wiederherstellung geht das wiederhergestellte Betriebssystem automatisch online.

Sollte eine Maschine nicht mehr booten können oder Sie ein System auf fabrikneue Hardware wiederherstellen müssen, dann booten Sie die Maschine mit einem bootfähigen Medium und konfigurieren Sie dort die Wiederherstellungsaktion auf die gleiche Art wie den Recovery-Task.



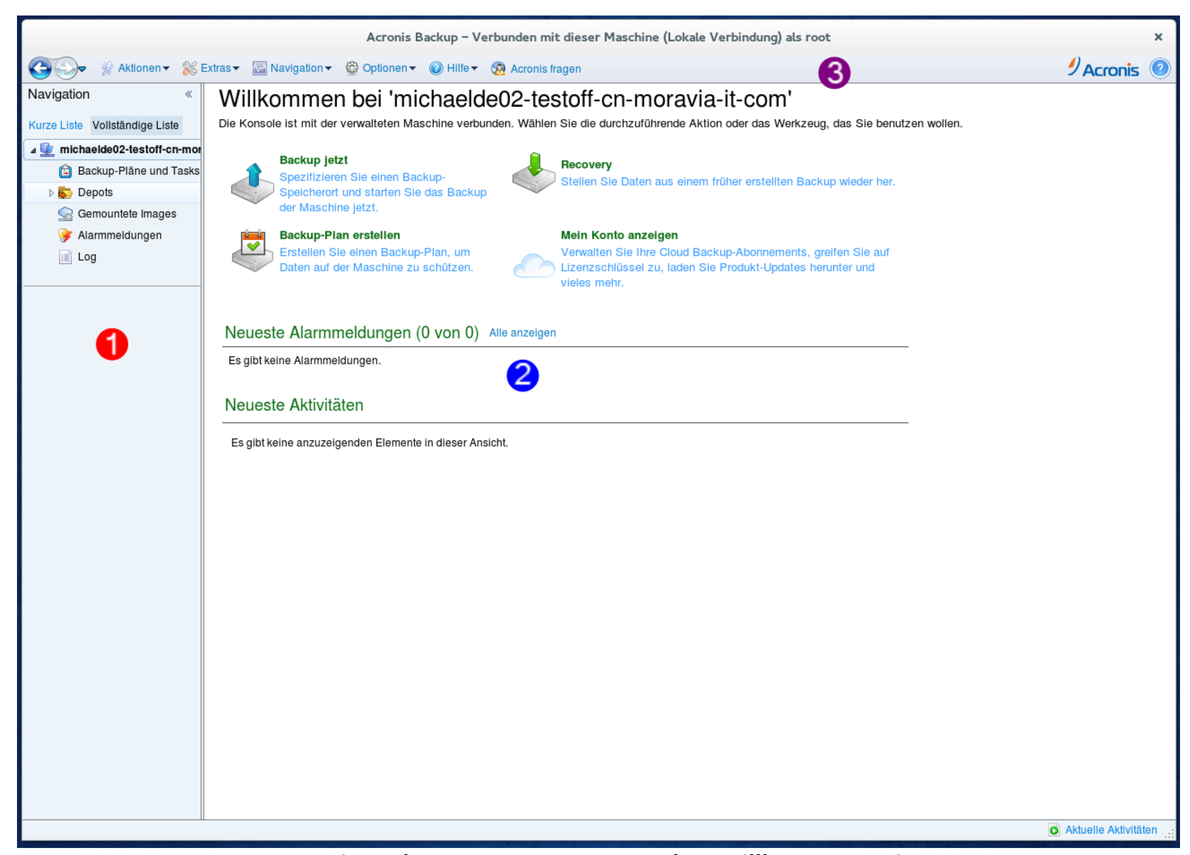
Schritt 6: Verwaltung

Der Fensterbereich **Navigation** (im linken Bereich der Konsole) ermöglicht Ihnen, zwischen den Produktansichten zu navigieren, die verschiedenen administrativen Zwecken dienen.

- Verwenden Sie die Anzeige **Backup-Pläne und Tasks**, um Backup-Pläne und Tasks zu verwalten: Sie können hier Tasks ausführen, bearbeiten, stoppen und löschen sowie ihre Stadien und ihren Fortschritt einsehen.
- Verwenden Sie die Anzeige **Alarmmeldungen**, um Probleme schnell erkennen und lösen zu können.
- Verwenden Sie die Anzeige **Logs**, um die Ereignismeldungen von Aktionen einzusehen.
- Der Ort, an dem Sie Ihre Backup-Dateien speichern, wird Depot (S. 298) genannt. Wechseln Sie zur Anzeige **Depots** (S. 162), um Informationen über Ihre Depots zu erhalten. Navigieren Sie von dort aus weiter zu dem gewünschten Depot, um Backups und ihre Inhalte einzusehen. Sie können Daten für eine Wiederherstellung auswählen und diverse manuelle Aktionen mit Backups durchführen (mounten, validieren, löschen etc.).

2.1 Die Management Konsole verwenden

Sobald die Konsole startet, werden die entsprechenden Elemente in der gesamten Arbeitsumgebung der Konsole angezeigt (im Menü, im Hauptbereich mit der **Willkommensseite** oder im Fensterbereich **Navigation**), wodurch Ihnen ermöglicht wird, maschinenspezifische Aktionen durchzuführen.



Acronis Backup Management Console – Willkommensseite

Wichtige Elemente der Arbeitsfläche der Konsole

	Name	Beschreibung
1	Fensterbereich **Navigation**	Enthält den Verzeichnisbaum **Navigation**. Ermöglicht Ihnen eine Navigation zwischen unterschiedlichen Ansichten. Weitere Informationen finden Sie unter Fensterbereich 'Navigation' (S. 16).
2	Hauptbereich	Sie können hier Backup-, Recovery- und andere Aktionen konfigurieren und überwachen. Die im Hauptbereich angezeigten Ansichten und Aktionsseiten (S. 17) hängen von den Elementen ab, die im Menü oder Verzeichnisbaum **Navigation** ausgewählt wurden.
3	**Menüleiste**	Wird quer über den oberen Bereich des Programmfensters angezeigt. Ermöglicht Ihnen, die gängigsten Aktionen von Acronis Backup auszuführen. Die Menüelemente ändern sich dynamisch, abhängig vom im Verzeichnisbaum **Navigation** und im Hauptbereich ausgewählten Element.

2.1.1 Fensterbereich 'Navigation'

Der Fensterbereich 'Navigation' enthält den Verzeichnisbaum **Navigation**.

Verzeichnisbaum 'Navigation'

Mit Hilfe des Verzeichnisbaums **Navigation** können Sie sich durch die Programmansichten bewegen. Sie können für die Ansichten zwischen **Vollständige Liste** oder **Kurze Liste** wählen. Die **Kurze Liste** enthält die am häufigsten verwendeten Ansichten der **Vollständigen Liste**.

Die Anzeige der **Kurzen Liste** enthält

- **[Name der Maschine]**. Die oberste Ebene des Verzeichnisbaums, auch **Willkommensseite** genannt. Hier wird der Name der Maschine angezeigt, mit der die Konsole momentan verbunden ist. Verwenden Sie diese Ansicht, um schnell auf wichtige Aktionen zuzugreifen, die auf der verwalteten Maschine verfügbar sind.
    - **Backup-Pläne und Tasks**. Verwenden Sie diese Ansicht, um Backup-Pläne und Tasks auf der verwalteten Maschine zu verwalten: Sie können Tasks hier ausführen, bearbeiten, stoppen und löschen sowie ihren Fortschritt einsehen.
    - **Depots**. Verwenden Sie diese Ansicht, um persönliche Depots und darin gespeicherte Archive zu verwalten, neue Depots hinzuzufügen, bestehende Depots umzubenennen oder zu löschen, Depots zu validieren, Backup-Inhalte zu untersuchen, Aktionen auf Archive und Backups anzuwenden usw.
    - **Alarmmeldungen**. Verwenden Sie diese Ansicht, um Warnmeldungen für die verwaltete Maschine zu untersuchen.

Die Anzeige der **Vollständigen Liste** enthält zusätzlich

- **Laufwerksverwaltung**. Verwenden Sie diese Ansicht, um Aktionen mit den Festplatten und ähnlichen Laufwerken einer Maschine auszuführen.
- **Log**. Verwenden Sie diese Ansicht, um Informationen zu solchen Aktionen zu überprüfen, die vom Programm auf der verwalteten Maschine ausgeführt werden.
- **Gemountete Images**. Dieser Knoten wird angezeigt, wenn mindestens ein Volume gemountet ist. Verwenden Sie diese Ansicht, um gemountete Images zu verwalten.

Aktionen mit den Fensterbereichen

So erweitern/minimieren Sie Fensterbereiche

Der Fensterbereich **Navigation** erscheint standardmäßig erweitert. Möglicherweise müssen Sie den Fensterbereich minimieren, um sich zusätzliche freie Arbeitsfläche zu verschaffen. Klicken Sie dazu auf das entsprechende Chevron-Symbol (). Der Fensterbereich wird daraufhin minimiert und das Chevron-Symbol ändert seine Orientierung (). Klicken Sie ein weiteres Mal auf das Chevron-Symbol, um den Fensterbereich zu erweitern.

So ändern Sie die Begrenzungen der Fensterbereiche.

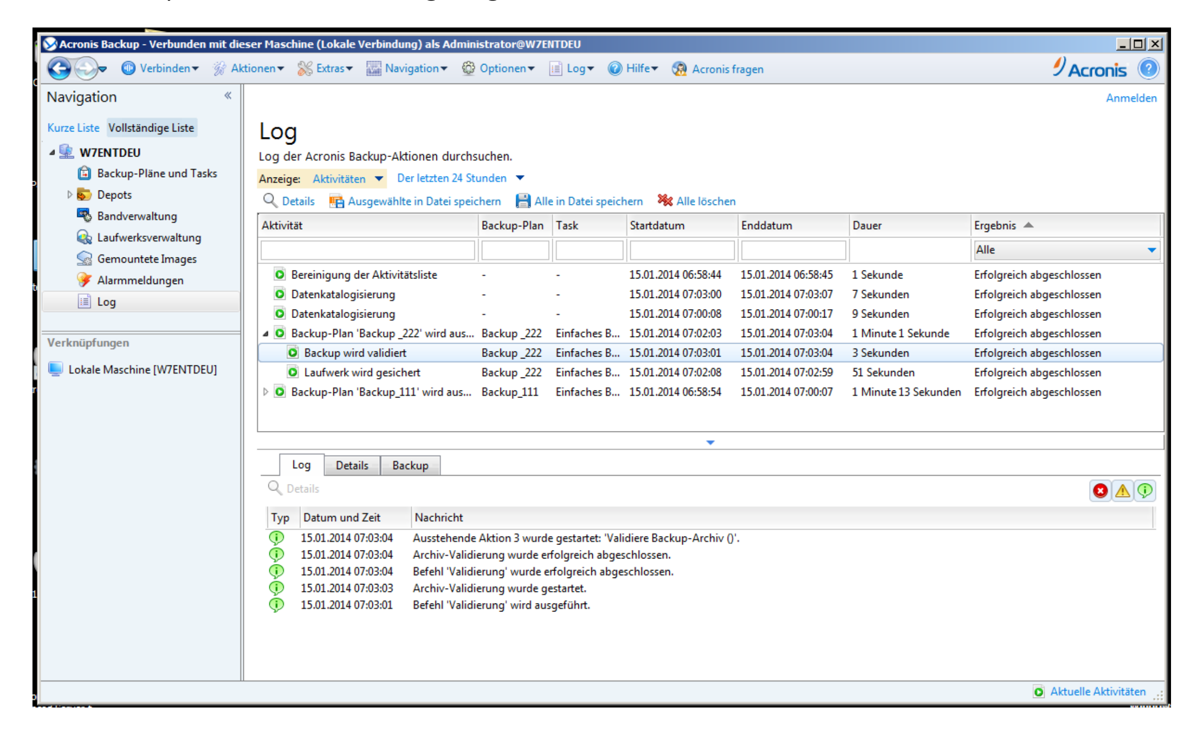
1. Zeigen Sie auf die Begrenzungslinie des Fensterbereiches.
2. Wenn der Zeiger als Pfeil mit zwei Spitzen angezeigt wird, dann ziehen Sie, um den Rand zu verschieben.

2.1.2 Hauptfenster, Ansichten und Aktionsseiten

Das Hauptfenster ist der zentrale Bereich, in dem Sie mit der Konsole arbeiten. Sie können Backup-Pläne und Recovery-Tasks erstellen, bearbeiten und verwalten sowie andere Aktionen ausführen. Die im Hauptbereich angezeigten Ansichten und Aktionsseiten hängen von den Elementen ab, die Sie im Menü oder im Verzeichnisbaum **Navigation** auswählen.

2.1.2.1 Ansichten

Wenn Sie auf ein beliebiges Element im **Navigationsbaum** der Seitenleiste Navigation (S. 16) klicken, wird eine entsprechende Ansicht angezeigt.



Ansicht „Log“

Übliche Arbeitsweise mit Ansichten

In der Regel enthält jede Ansicht eine Tabelle mit Elementen, eine Symbolleiste mit Schaltflächen für die Tabelle sowie den unteren Fensterbereich **Informationen**.

- Verwenden Sie die Funktionen zum Filtern und Sortieren (S. 18), um die Tabelle nach dem gewünschten Element zu durchsuchen.
- Wählen Sie in der Tabelle das gewünschte Element aus.
- Sehen Sie sich im Fensterbereich Informationen (standardmäßig eingeklappt) die Details des Elements an. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol ▲ klicken.
- Führen Sie die entsprechenden Aktionen mit dem ausgewählten Element aus. Es gibt verschiedene Möglichkeiten, wie Sie ein und dieselbe Aktion mit ausgewählten Elementen ausführen können:
  - Indem Sie auf die Schaltflächen in der Symbolleiste der Tabelle klicken.
  - Indem Sie die Elemente im Menü **Aktionen** wählen.
  - Indem Sie mit der rechten Maustaste auf das Element klicken und die Aktion im Kontextmenü auswählen.

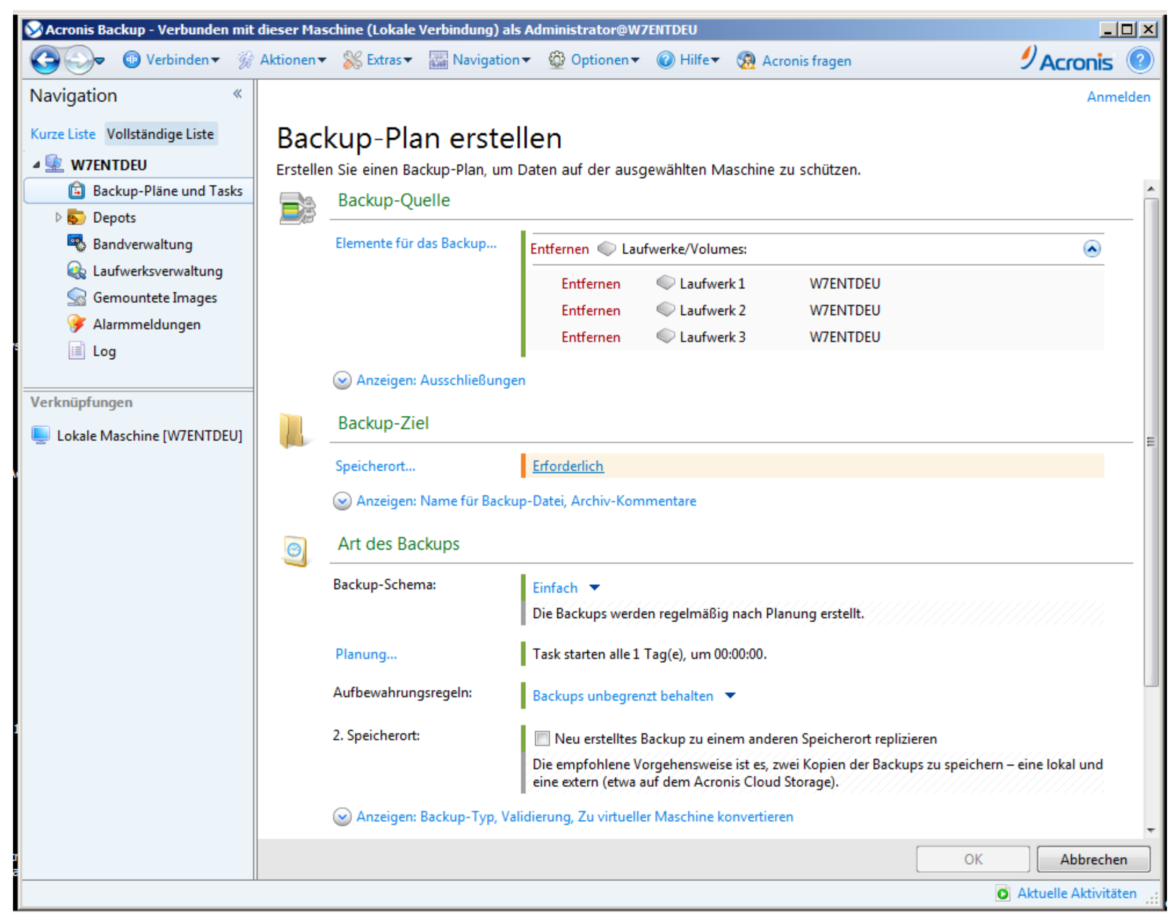
Tabellenelemente sortieren, filtern und konfigurieren

Nachfolgend finden Sie eine Anleitung, wie Sie Tabellenelemente in jeder Ansicht sortieren, filtern und konfigurieren können.

Aufgabe	Tun Sie Folgendes
Elemente nach Spalten sortieren	Klicken Sie auf einen Spaltenkopf, um die Elemente aufsteigend sortieren zu lassen. Kicken Sie erneut auf den Spaltenkopf, um die Elemente in absteigender Reihenfolge sortieren zu lassen.
Elemente nach einem vordefinierten Spaltenwert filtern	Wählen Sie in einem Feld unter der entsprechenden Spaltenkopf den gewünschten Wert aus dem Listenfeld.
Elemente nach einem eingegebenen Wert filtern	Geben Sie in einem Feld unter dem entsprechenden Spaltenkopf einen Wert ein. Als Ergebnis sehen Sie eine Liste von Werten, die vollständig oder teilweise mit dem eingegebenen Wert übereinstimmen.
Elemente nach vordefinierten Parametern filtern	Klicken Sie auf die entsprechenden Schaltflächen über der Tabelle. Sie können beispielsweise in der Ansicht **Log** die Log-Einträge nach dem Ereignistyp filtern (Information, Warnung, Fehler) oder nach dem Zeitraum, in dem das Ereignis auftrat (**Der letzten 24 Stunden**, **Der letzten Woche**, **Der letzten 3 Monate** oder **Benutzerdefinierter Zeitraum**).
Tabellenspalten anzeigen oder verbergen	Standardmäßig hat jede Tabelle eine bestimmte Anzahl von angezeigten Spalten, während andere verborgen sind. Sie können nicht benötigte Spalten außerdem ausblenden bzw. ausgeblendete anzeigen lassen. Spalten anzeigen oder verbergen 1. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um das Kontextmenü zu öffnen. 2. Klicken Sie auf die Elemente, die Sie anzeigen bzw. verbergen wollen.

2.1.2.2 Aktionsseiten

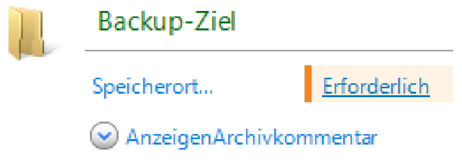
Wenn Sie im Menü **Aktionen** auf ein Element klicken, erscheint im Hauptbereich eine Aktionsseite. Diese enthält Schritte, die Sie ausführen müssen, um einen beliebigen Task oder einen Backup-Plan zu erstellen und zu starten.



Aktionsseite – Backup-Plan erstellen

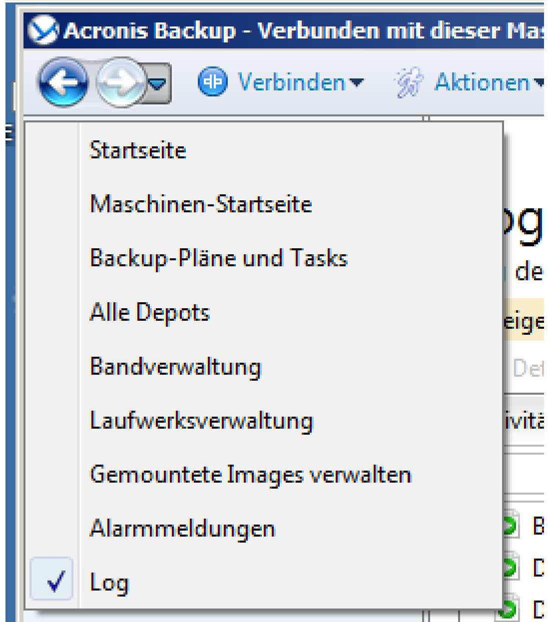
Steuerelemente verwenden und Einstellungen festlegen

Verwenden Sie die aktiven Steuerelemente, um die Einstellungen und Parameter eines Backup-Plans oder Recovery-Tasks zu spezifizieren. Standardmäßig handelt es sich bei diesen Feldern um Anmeldedaten, Optionen, Kommentare und einige andere, verborgene. Die meisten Einstellungen werden konfiguriert, indem Sie auf die entsprechenden Links **Anzeigen…** klicken. Andere Einstellungen werden aus einem Listenfeld ausgewählt oder manuell in die Felder auf der Seite eingegeben.



Aktionsseite – Steuerelemente

Acronis Backup merkt sich die Änderungen, die Sie auf den Aktionsseiten vornehmen. Wenn Sie z.B. begonnen haben, einen Backup-Plan zu erstellen und dann aus irgendeinem Grund zu einer anderen Ansicht gewechselt sind, ohne die Plan-Erstellung abzuschließen, können Sie die Navigationsschaltfläche **Zurück** im Menü anklicken. Oder, wenn Sie bereits mehrere Schritte vorwärts gegangen sind, klicken Sie den Pfeil **Nach unten** und wählen die Seite, auf der Sie die Plan-Erstellung aus der Liste gestartet haben. Auf diese Weise können Sie die verbleibenden Schritte ausführen und die Erstellung des Backup-Plans abschließen.



Navigationsschaltflächen

2.1.3 Konsolen-Optionen

Die Konsolenoptionen legen fest, wie die Informationen in der grafischen Benutzeroberfläche von Acronis Backup erscheinen.

Um auf die Konsolenoptionen zuzugreifen, wählen Sie **Optionen -> Konsolenoptionen** im Menü.

2.1.3.1 Optionen für Alarmanzeige

Die Option spezifiziert, welche Alarmmeldungen in der Ansicht **Alarmmeldungen** angezeigt bzw. verborgen werden sollen.

Voreinstellung ist: **Alle Alarmmeldungen**.

Um Alarmmeldungen anzuzeigen (zu verbergen), (de)aktivieren Sie die Kontrollkästchen neben den entsprechenden Alarmtypen.

2.1.3.2 Anmeldedaten zwischenspeichern

Diese Option spezifiziert, ob die bei Verwendung der Management Konsole eingegebenen Anmeldedaten gespeichert werden sollen.

Voreinstellung ist: **Aktiviert**.

Ist die Option aktiviert, dann werden die von Ihnen während einer Konsolensitzung für verschiedene Speicherorte eingegebenen Anmeldedaten zur Nutzung in späteren Sitzungen gespeichert. Unter Windows werden die Anmeldedaten in der Anmeldeinformationsverwaltung (Windows Credentials Manager) gespeichert. Unter Linux werden die Anmeldedaten in einer speziellen, verschlüsselten Datei gespeichert.

Ist die Option deaktiviert, dann werden die Anmeldedaten nur solange zwischengespeichert, bis die Konsole geschlossen wird.

Um die für das aktuelle Benutzerkonto zwischengespeicherten Anmeldedaten zu löschen, klicken Sie auf die Schaltfläche **Cache für Anmeldedaten bereinigen**.

2.1.3.3 Schriftarten

Die Option legt fest, welche Schriftarten in der grafischen Benutzeroberfläche von Acronis Backup erscheinen. Die Einstellung **Menü-Schriftart** beeinflusst die Dropdown- und Kontextmenüs. Die Einstellung **Anwendung-Schriftart** beeinflusst alle anderen Benutzeroberflächenelemente.

Voreinstellung ist: **Systemstandardschriftart** sowohl für die Menüs als für die Schnittstellenelemente der Anwendung.

Um eine Auswahl zu treffen, wählen Sie die Schriftart im jeweiligen Listenfeld und stellen die Schrifteigenschaften ein. Sie können eine Vorschau der Schriftenanzeige erhalten, wenn Sie rechts daneben auf **Durchsuchen** klicken.

2.1.3.4 Pop-up-Meldungen

Über Tasks, die einen Benutzereingriff erfordern

Diese Option ist wirksam, wenn die Konsole mit einer verwalteten Maschine verbunden ist.

Die Option legt fest, ob das Pop-up-Fenster erscheint, wenn ein oder mehrere Tasks eine Interaktion erfordern. Dieses Fenster ermöglicht Ihnen, für alle Tasks am selben Platz eine Entscheidung zu treffen, wie z.B. einen Neustart zu bestätigen oder einen Neuversuch nach Freigabe von Festplattenplatz zu erlauben. So lange wenigstens ein Task eine Interaktion erfordert, können Sie dieses Fenster jederzeit vom **Dashboard** der verwalteten Maschine öffnen. Alternativ können Sie die Ausführungsstadien des Tasks in der Ansicht **Tasks** überprüfen und Ihre Entscheidung für jeden Task im Bereich **Information** treffen.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, benutzen Sie das Kontrollkästchen **Fenster „Tasks erfordern Benutzereingriff" anzeigen**.

Über Ergebnisse der Task-Ausführung

Diese Option ist nur wirksam, wenn die Konsole mit einer verwalteten Maschine verbunden ist.

Die Option legt fest, ob die Pop-up-Meldungen über Ergebnisse der Task-Ausführung erscheinen: Erfolgreiche Vollendung, Fehlschlagen oder erfolgreicher Abschluss mit Warnungen. Wenn die Anzeige der Pop-up-Meldungen deaktiviert ist, können Sie die Ausführungsstadien und Ergebnisse des Tasks in der Ansicht **Tasks** überprüfen.

Voreinstellung ist: **Aktiviert** für alle Ergebnisse.

Um eine Einstellung für jedes Ergebnis ('Erfolgreiche Vollendung', 'Fehlschlagen' oder 'Erfolgreicher Abschluss mit Warnungen') einzeln festzulegen, benutzen Sie das zugehörige Kontrollkästchen.

3 Acronis Backup verstehen

Dieser Abschnitt bemüht sich, den Lesern ein klareres, vertieftes Verständnis des Produktes zu vermitteln, damit es sich auch ohne Schritt-für-Schritt-Anleitungen unter den unterschiedlichsten Umständen erfolgreich einsetzen lässt.

3.1 Besitzer

In diesem Abschnitt wird das Konzept von Backup-Plan-/Task-Besitzern und Archiv-Besitzern erklärt.

Plan- oder Task-Besitzer

Ein lokaler Backup-Plan-Besitzer ist derjenige Benutzer, der den Plan erstellt oder als letzter verändert hat.

Tasks, die Bestandteil eines Backup-Plans sind, gehören einem Backup-Plan-Besitzer.

Tasks, die kein Bestandteil eines Backup-Plans sind (wie z.B. Recovery-Tasks), gehören dem Benutzer, der den Task erstellt oder als letzter modifiziert hat.

Einen Plan (Task) verwalten, der einem anderen Benutzer gehört

Ein Benutzer, der auf einer Maschine administrative Berechtigungen hat, kann die Tasks und lokalen Backup-Pläne eines jeden Benutzers, der im Betriebssystem registriert ist, verändern.

Wenn ein Benutzer einen Plan oder Task, der einem anderen Benutzer gehört, zur Bearbeitung öffnet, werden alle in diesem Task gesetzten Passwörter gelöscht. Das verhindert ein Vorgehen „verändere die Einstellungen, behalte Passwörter". Das Programm reagiert jedes Mal mit einer Warnung, wenn Sie versuchen, einen Plan (Task) zu editieren, den zuletzt ein anderer Benutzer modifiziert hat. Wenn Sie die Warnung sehen, haben Sie zwei Möglichkeiten:

- Klicken Sie auf **Abbrechen** und erstellen Sie einen eigenen Plan oder Task. Der ursprüngliche Task bleibt dabei intakt.
- Fahren Sie mit dem Editieren fort. In dem Fall müssen Sie alle zur Ausführung des Plans oder Tasks benötigten Anmeldedaten eingeben.

Archiv-Besitzer

Ein Archiv-Besitzer ist der Benutzer, der das Archiv am Zielort gespeichert hat. Präziser gesagt ist es derjenige Anwender, dessen Konto bei Erstellung des Backup-Plans im Schritt **Backup-Ziel festlegen** angegeben wurde. Standardmäßig werden die Anmeldedaten des Backup-Plans verwendet.

3.2 In Backup-Plänen und Tasks verwendete Anmeldedaten

Dieser Abschnitt erläutert das Konzept von Zugriffsanmeldedaten, Anmeldedaten für Backup-Pläne und Anmeldedaten für Tasks.

Anmeldedaten

Sie müssen beim Durchsuchen von Backup-Speicherorten, der Einrichtung von Backups oder der Erstellung von Recovery-Tasks möglicherweise Anmeldedaten bereitstellen, um auf unterschiedliche

Ressourcen zugreifen zu können. Dazu gehören z. B. die Daten, die Sie per Backup sichern wollen oder der Speicherort, wo die Backups gespeichert sind (oder gespeichert werden sollen).

Falls die Option **Anmeldedaten zwischenspeichern** (S. 21) aktiviert ist (standardmäßig aktiviert), werden die von Ihnen während einer Konsolensitzung bereitgestellten Anmeldedaten zur Verwendung in späteren Sitzungen gespeichert. Sie müssen die Anmeldedaten daher beim nächsten Mal nicht erneut eingeben. Die Anmeldedaten werden für jeden Besitzer, der die Konsole auf der Maschine verwendet, unabhängig zwischengespeichert.

Anmeldedaten des Backup-Plans

Jeder Backup-Plan, der auf einer Maschine läuft, läuft im Namen eines bestimmten Benutzers.

In Windows:

Der Plan läuft standardmäßig unter dem Konto des Agenten-Dienstes (Agent Service), sofern er durch einen Benutzer erstellt wurde, der auf der Maschine administrative Berechtigungen hat. Falls er durch einen normalen Benutzer erstellt wurde, etwa einem Mitglied der Gruppe **Benutzer**, dann läuft der Plan unter dem Konto dieses Benutzers.

Sie werden bei Erstellung eines Backup-Plans nur in bestimmten Fällen nach Anmeldedaten gefragt. Beispielsweise:

- Sie planen Backups als ein normaler Benutzer und haben bei Verbindung der Konsole mit der Maschine keine Anmeldedaten eingegeben. Dies kann der Fall sein, wenn die Konsole auf derselben Maschine installiert ist, die Sie per Backup sichern.
- Sie sichern einen Microsoft Exchange-Cluster per Backup zu einem Storage Node.

Die Anmeldedaten explizit spezifizieren

Sie haben die Möglichkeit, explizit ein bestimmtes Benutzerkonto zu spezifizieren, unter dem der Backup-Plan ausgeführt wird. So gehen Sie auf der Seite zur Backup-Plan-Erstellung vor:

1. Klicken Sie im Bereich **Plan-Parameter** auf **Anmeldedaten des Plans, Kommentare, Bezeichnung anzeigen**.
2. Klicken Sie auf **Anmeldedaten des Plans**.
3. Geben Sie die Anmeldedaten ein, unter denen der Plan laufen soll. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.

In Linux:

Sie müssen keine Anmeldedaten für Backup-Pläne spezifizieren. Unter Linux laufen Backup-Pläne immer unter dem Benutzerkonto 'root'.

Anmeldedaten für den Task

Wie ein Backup-Plan läuft auch jeder Task im Namen eines bestimmten Benutzers.

In Windows:

Beim Erstellen eines Tasks haben Sie die Möglichkeit, explizit ein Konto anzugeben, unter dem der Task laufen wird. Ihre Wahl hängt davon ab, ob die Ausführung des Tasks manuell oder zeit- bzw. ereignisgesteuert erfolgen soll.

- **Manueller Start**

  Jedes Mal, wenn Sie einen Task manuell starten, wird er mit den Anmeldedaten ausgeführt, mit denen Sie zu der Zeit am System angemeldet sind. Außerdem kann der Task auch von jeder

Person, die auf der Maschine über administrative Rechte verfügt, gestartet werden. Der Task wird dann unter den Anmeldedaten dieser Person ausgeführt.

Für den Fall, dass Sie die Anmeldedaten für einen Task explizit spezifizieren, wird er auch immer mit genau diesen ausgeführt, unabhängig davon, welcher Anwender den Task dann tatsächlich startet.

- **Zeit-/ereignisgesteuerter oder verschobener Start**

  Anmeldedaten für den Task sind zwingend. Sie können die Task-Erstellung nicht abschließen, bevor Sie die Anmeldedaten für den Task spezifiziert haben. Anmeldedaten für den Task werden auf der Seite zur Task-Erstellung in ähnlicher Weise wie die Anmeldedaten für den Plan spezifiziert.

In Linux:

Sie müsse keine Anmeldedaten für Tasks spezifizieren. Unter Linux laufen Tasks immer unter dem Benutzerkonto 'root'.

3.3 Benutzerberechtigungen auf einer verwalteten Maschine

Der Umfang an Rechten, den ein Benutzer bei Verwaltung einer unter Windows laufenden Maschine hat, hängt von seinen allgemeinen Benutzerberechtigungen auf der jeweiligen Maschine ab.

Normale Benutzer

Ein normaler Benutzer, wie es etwa ein Mitglied der Gruppe 'Benutzer' ist, verfügt über folgende Verwaltungsrechte:

- Durchführung von Backup und Wiederherstellung auf Datei-Ebene, mit Dateien, auf die der Benutzer Zugriffsrechte hat – jedoch ohne Nutzung von Backup-Snapshots auf Datei-Ebene (S. 99).
- Backup-Pläne und Tasks erstellen und diese verwalten
- Die Backup-Pläne und Tasks anderer Nutzer können eingesehen, jedoch nicht verwaltet werden.
- Einsicht in die lokale Ereignisanzeige

Sicherungs-Operatoren

Ein Benutzer, der Mitglied der Gruppe 'Sicherungs-Operatoren' ist, hat folgendes Verwaltungsrecht:

- Backup und Wiederherstellung der kompletten Maschine oder von beliebigen Daten auf der Maschine, mit oder ohne Laufwerk-Snapshot Die Verwendung eines Hardware Snapshot Providers kann immer noch administrative Berechtigungen erfordern.

Administratoren

Ein Benutzer, der Mitglied der Gruppe 'Administratoren' ist, hat folgendes Verwaltungsrecht:

- Backup-Pläne und Tasks, die anderen Benutzern auf der Maschine gehören, einsehen und verwalten.

3.4 Liste der Acronis Services (Dienste)

Acronis Backup erstellt während der Installation mehrere Dienste. Einige dieser Dienste können auch von anderen auf der Maschine installierten Acronis-Produkten verwendet werden.

Die Dienste von Acronis Backup

Die Dienste umfassen den Hauptdienst (Main Service) und eine Anzahl von Hilfsdiensten (Auxiliary Services).

Der Hauptdienst kann unter einem dedizierten Konto laufen oder einem von Ihnen spezifizierten Konto (während der Installation). Beiden Konten werden Berechtigungen gegeben, die erforderlich sind, damit der Dienst arbeiten kann. Diese Berechtigungen beinhalten eine Zusammenstellung von Benutzerrechten, Mitgliedschaft in Sicherheitsgruppen und die Erlaubnis zum **Vollzugriff** auf Registry-Einträge in folgendem Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis. Es werden keine weiteren Berechtigungen für andere Registry-Schlüssel gewährt.

Die folgende Tabelle listet die Dienste von Acronis Backup und die Berechtigungen für ihre Konten auf.

<table>
<tr><th rowspan="2">Name des Dienstes</th><th rowspan="2">Zweck</th><th rowspan="2">Vom Dienst verwendetes Konto</th><th colspan="3">Dem Konto hinzugefügte Berechtigungen</th></tr>
<tr><th>Benutzerrechte</th><th>Gruppenmit-gliedschaft</th><th>Berechtigungen für Registry-Schlüssel</th></tr>
<tr><td>Acronis Managed Machine Service
(Hauptdienst)</td><td>Backup und Recovery von Daten auf der Maschine</td><td>Acronis Agent User (neues Konto) oder benutzer-spezifiziertes Konto</td><td>Als Dienst anmelden
Anpassen von Speicherkon-tingenten für einen Prozess
Ersetzen eines Token auf Prozessebene
Verändern der Firmwareumge-bungsvariablen</td><td>Sicherungs-Operatoren (für jedes Konto)
Administratoren (nur für ein neues Konto)</td><td>BackupAnd-Recovery
Verschlüsselung
Global
MMS</td></tr>
<tr><td>Acronis VSS Provider
(Hilfsdienst; nur unter Windows Server-Betriebs-systemen erstellt)</td><td>Verwendung eines Volume Shadow Copy (VSS) Providers (S. 109) (Volumenschat-tenkopie-Anbieter), der mit Acronis Backup ausgeliefert wird.</td><td>Lokales System</td><td colspan="3">Keine zusätzlichen Berechtigungen</td></tr>
<tr><td>Acronis Removable Storage Management Service
(Hilfsdienst)</td><td>Verwaltung lokal angeschlossener Bandgeräte</td><td>Lokales System</td><td colspan="3">Keine zusätzlichen Berechtigungen</td></tr>
</table>

Allgemeine Dienste für Acronis Backup und andere Acronis-Produkte

Folgende Dienste werden können gemeinsam mit anderen auf der Maschine installierten Acronis-Produkten verwendet werden. Diese Dienste laufen unter einem Systemkonto. Dem Konto werden keine zusätzlichen Berechtigungen gegeben.

Name des Dienstes	Zweck	Vom Dienst verwendetes Konto
Acronis Remote Agent Service	Stellt die Verbindungsmöglichkeit zwischen Acronis-Komponenten bereit.	**Lokales System** (Windows Vista und später) oder **NetworkService** (früher als Windows Vista)
Acronis Scheduler2 Service	Ermöglicht die Planung von durch Acronis-Komponenten durchgeführte Tasks.	**Lokales System**

Abhängigkeiten von anderen Diensten

Der Acronis Managed Machine Service hängt von folgenden Windows-Standard-Diensten ab: **Remoteprozeduraufruf (RPC)**, **Geschützter Speicher** und **Windows-Verwaltungsinstrumentation**. Dieser Dienst hängt außerdem vom Acronis Scheduler2 Service ab.

Gehen Sie folgendermaßen vor, um eine Liste der Abhängigkeiten für einen Dienst einzusehen:

1. Klicken Sie im Snap-in **Dienste** doppelt auf den Namen des Dienstes.
2. Betrachten Sie in der Registerkarte **Abhängigkeiten** das Feld **Dieser Dienst ist von diesen Systemkomponenten abhängig...**.

3.5 Vollständige, inkrementelle und differentielle Backups

Acronis Backup ermöglicht Ihnen, gängige Backup-Schemata (z.B. Großvater-Vater-Sohn oder „Türme von Hanoi“) wie auch selbst erstellte Schemata zu verwenden. Alle Backup-Schemata basieren auf vollständigen, inkrementellen und differentiellen Backup-Methoden. Genau genommen kennzeichnet der Begriff „Schemata“ den Algorithmus zur Anwendung dieser Methoden plus dem Algorithmus zur Backup-Bereinigung.

Backup-Methoden miteinander zu vergleichen macht nicht viel Sinn, da die Methoden als Team in einem Backup-Schema arbeiten. Jede Methode sollte abhängig von ihren Vorteilen ihre spezifische Rolle spielen. Ein sachgerechtes Backup-Schema profitiert von den Vorteilen und vermindert die Unzulänglichkeiten aller Backup-Methoden. So erleichtert z.B. ein wöchentliches differentielles Backup eine Archiv-Bereinigung, da es zusammen mit einem wöchentlichen Set täglicher, von ihm abhängender inkrementeller Backups mühelos gelöscht werden kann.

Mit vollständigen, inkrementellen oder differentiellen Backup-Methoden durchgeführte Sicherungen resultieren in Backups (S. 294) des jeweils entsprechenden Typs.

Voll-Backup

Ein vollständiges Backup speichert alle für ein Backup ausgewählten Daten. Ein Voll-Backup liegt jedem Archiv zugrunde und bildet die Basis für inkrementelle und differentielle Backups. Ein Archiv kann mehrere Voll-Backups enthalten oder nur aus Voll-Backups bestehen. Ein Voll-Backup ist autark – Sie benötigen also keinen Zugriff auf irgendein anderes Backup, um Daten aus diesem Voll-Backup wiederherzustellen.

Es ist weitgehend akzeptiert, dass ein Voll-Backup bei der Erstellung am langsamsten, aber bei der Wiederherstellung am schnellsten ist. Eine Wiederherstellung aus einem inkrementellen Backup ist dank Acronis-Technologien jedoch nicht langsamer als aus einem vollständigen Backup.

Ein Voll-Backup ist am nützlichsten, wenn:

- Sie ein System auf seinen Ausgangszustand zurückbringen wollen
- dieser Ausgangszustand sich nicht häufig ändert, so dass es keine Notwendigkeit für reguläre Backups gibt.

Beispiel: Ein Internet-Cafe, eine Schule oder ein Universitätslabor, wo der Administrator durch Studenten oder Gäste bewirkte Änderungen rückgängig macht, aber nur selten das Referenz-Backup aktualisiert (tatsächlich nur nach Installation neuer Software). In diesem Fall ist der Backup-Zeitpunkt nicht entscheidend, während die zur Wiederherstellung aus dem Voll-Backup benötigte Zeit minimal ist. Zur Erreichung einer zusätzlichen Ausfallsicherheit kann der Administrator mehrere Kopien des Voll-Backups haben.

Inkrementelles Backup

Ein inkrementelles Backup speichert die Veränderungen der Daten in Bezug auf das **letzte Backup**. Sie benötigen Zugriff auf die anderen Backups des gleichen Archivs, um Daten aus einem inkrementellen Backup wiederherzustellen.

Ein inkrementelles Backup ist am nützlichsten, wenn:

- es möglich sein muss, die Daten zu jedem der multiplen, gespeicherten Zustände zurückzusetzen.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Es ist weitgehend akzeptiert, dass inkrementelle Backups weniger zuverlässig als Voll-Backups sind, da bei Beschädigung eines Backups innerhalb der „Kette“ auch die nachfolgenden nicht mehr verwendet werden können. Dennoch ist das Speichern mehrerer Voll-Backups keine Option, wenn Sie multiple frühere Versionen Ihrer Daten benötigen, da die Verlässlichkeit eines übergroßen Archivs noch fragwürdiger ist.

Beispiel: Das Backup eines Datenbank-Transaktions-Logs.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum **letzten Voll-Backup**. Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen. Ein differentielles Backup ist am nützlichsten, wenn:

- Sie daran interessiert sind, nur den neusten Datenzustand zu speichern.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Die typische Schlussfolgerung ist: Differentielle Backups sind langsamer bei Erstellung, aber schneller bei Wiederherstellung, während inkrementelle schneller zu erstellen, aber langsamer wiederherzustellen sind. Tatsächlich gibt es keinen physikalischen Unterschied zwischen einem an ein Voll-Backup angefügten, inkrementellen Backup und einem differentiellen Backup, welches demselben Voll-Backup zum gleichen Zeitpunkt angehängt wird. Der weiter oben erwähnte Unterschied setzt die Erstellung eines differentiellen Backups nach (oder statt) Erstellung multipler differentieller Backups voraus.

Ein nach Defragmentierung einer Festplatte erstelltes inkrementelles oder differentielles Backup kann beträchtlich größer als üblich sein, weil die Defragmentierung die Speicherposition von Dateien auf der Platte verändert und die Backups genau diese Veränderungen reflektieren. Es wird daher empfohlen, dass Sie nach einer Festplatten-Defragmentierung erneut ein Voll-Backup erstellen.

Die nachfolgende Tabelle fasst die allgemein bekannten Vorteile und Schwächen jedes Backup-Typs zusammen. Unter realen Bedingungen hängen diese Parameter von zahlreichen Faktoren ab, wie Menge, Größe und Muster der Datenveränderungen, Art der Daten, den physikalischen Spezifikationen der Geräte, den von Ihnen eingestellten Backup- bzw. Recovery-Optionen und einigen mehr. Praxis ist der beste Leitfaden für die Wahl des optimalen Backup-Schemas.

Parameter	Voll-Backup	Differentielles Backup	Inkrementelles Backup
Speicherplatz	Maximal	Medium	Minimal
Erstellungszeit	Maximal	Medium	Minimal
Wiederherstellungszeit	Minimal	Medium	Maximal

3.6 Was speichert das Backup eines Laufwerks oder Volumes?

Ein Laufwerk- bzw. Volume-Backup speichert das **Dateisystem** des entsprechenden Laufwerks bzw. Volumes 'als Ganzes'. Dabei werden auch alle zum Booten des Betriebssystems erforderlichen Informationen eingeschlossen. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Windows

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die FAT (File Allocation Table) und – sofern vorhanden – auch das Stammverzeichnis (Root) und die Spur Null (Track Zero), inkl. Master Boot Record (MBR).

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und die Spur Null (Track Zero) mit dem Master Boot Record (MBR).

Folgende Elemente sind in einem Laufwerk- oder Volume-Backup nicht enthalten (und genauso wenig in einem Backup auf Dateiebene):

- Die Auslagerungsdatei (pagefile.sys) und die Datei, die ein Abbild des Hauptspeichers ist, wenn der Computer in den Ruhezustand wechselt (hiberfil.sys). Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.
- Windows Schattenspeicher (Shadow Storage). Der auf diesen verweisende Pfad wird über den Registry-Wert **VSS Default Provider** bestimmt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** gefunden werden kann. Das bedeutet, dass bei Betriebssystemen beginnend mit Windows Vista keine Systemwiederherstellungspunkte von Windows per Backup gesichert werden.

Linux

Ein Volume-Backup speichert alle Dateien und Verzeichnisse des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. der Spur Null (Track Zero) mit dem 'Master Boot Record' (MBR).

Bei aktivierter **'Sektor-für-Sektor'-Option (Raw-Modus)** werden alle Sektoren des Laufwerks im Laufwerk-Backup gespeichert. Das Sektor-für-Sektor-Backup kann verwendet werden, um Laufwerke

mit nicht erkannten oder nicht unterstützten Dateisystemen sowie anderen proprietären Datenformaten zu sichern.

3.7 Backup und Recovery von dynamischen Volumes (Windows)

Dieser Abschnitt erläutert in Kürze Backup und Wiederherstellung dynamischer Volumes (S. 300) durch Acronis Backup.

Ein dynamisches Volume ist ein Volume, das sich auf einem dynamischen Laufwerk (S. 299) oder genauer auf einer Laufwerksgruppe (S. 297) befindet. Acronis Backup unterstützt die folgenden dynamischen Laufwerkstypen/RAID-Level:

- Einfach/Übergreifend
- Stripeset (RAID 0)
- Gespiegelt (RAID 1)
- eine Stripeset-Spiegelung (RAID 0+1)
- RAID -5.

Dynamische Volumes werden gesichert

Dynamische Volumes werden auf gleiche Weise wie Volumes vom Typ 'Basis' gesichert. Beim Erstellen eines Backup-Plans über die Benutzeroberfläche stehen all diese Laufwerkstypen als **Backup-Objekte** zur Auswahl. Wenn Sie die Befehlszeileneingabe verwenden, so spezifizieren Sie dynamische Volumes mit dem Präfix 'DYN'.

Befehlszeilen-Beispiele

```
acrocmd backup disk --volume=DYN1,DYN2 --loc=\\srv1\backups
--credentials=netuser1,pass1 --arc=dyn1_2_arc
```

Dies erstellt ein Backup der Volumes DYN1 und DYN2 in einen freigegebenen Netzwerkordner.

```
acrocmd backup disk --volume=DYN --loc=\\srv1\backups --credentials=netuser1,pass1
--arc=alldyn_arc
```

Dies erstellt ein Backup aller dynamischen Volumes der lokalen Maschine zu einem freigegebenen Netzwerkordner.

Dynamische Volumes werden wiederhergestellt

Ein dynamisches Volume kann wiederhergestellt werden:

- Über jeden existierenden Volume-Typ.
- Auf dem 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe.
- Auf dem 'nicht zugeordneten' Speicherplatz eines Basis-Laufwerks.
- Auf einem noch nicht initialisierten Laufwerk.

Recovery über ein existierendes Laufwerk

Wenn ein dynamisches Laufwerk über ein existierendes Laufwerk ('Basis' oder 'dynamisch) wiederhergestellt wird, so werden die Daten des Ziellaufwerks mit dem Inhalt des Backups überschrieben. Der Typ des Ziellaufwerkes (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID -5) wird nicht verändert. Die Größe des Ziellaufwerkes muss ausreichend sein, um den Inhalt des Backups aufnehmen zu können.

Recovery zu nicht zugeordneten Speicherplatz einer Laufwerksgruppe

Wenn Sie ein dynamisches Volume zu dem 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe wiederherstellen, bewahrt die Software den Typ und die Größe des ursprünglichen Volumes. Sollte die Laufwerksgruppenkonfiguration den ursprünglichen Volume-Typ nicht erlauben, dann wird das Volume mit dem Typ 'Einfach' (Simple) oder 'Übergreifend' (Spanned) wiederhergestellt. Falls das Volume auf den 'nicht zugeordneten' Speicherplatz nicht passen sollte, dann erfolgt eine Größenanpassung des Volumes durch Verkleinerung seines freien Speicherplatzes.

Beispiele für Szenarien, in denen die Laufwerksgruppenkonfiguration den ursprünglichen Typ des Volumes nicht erlaubt

Beispiel 1. Die Gruppe enthält weniger Laufwerke als für das dynamische Volume erforderlich sind. Angenommen, Sie sind dabei, ein auf 3 Laufwerken liegendes RAID-5-Volume mit 80 GB auf eine Laufwerksgruppe wiederherzustellen, die aus zwei Laufwerken besteht. Die Gesamtgröße des 'nicht zugeordneten' Speicherplatzes beträgt 100 GB: 40 GB auf dem ersten Laufwerk und 60 GB auf dem zweiten. Das RAID-5-Volume wird als übergreifendes Volume (Spanned) über zwei Laufwerke wiederhergestellt.

Beispiel 2. Die Verteilung des 'nicht zugeordneten' Speicherplatzes erlaubt keine Wiederherstellung von dynamischen Volumes eines bestimmten Typs. Angenommen, Sie wollen ein 30 GB-Stripeset-Volume auf eine Laufwerksgruppe wiederherstellen, die aus zwei Laufwerken besteht. Die Gesamtgröße des 'nicht zugeordneten' Speicherplatzes beträgt 50 GB: 10 GB auf dem ersten Laufwerk und 40 GB auf dem zweiten. Das Stripeset-Volume wird mit dem Typ 'Einfach' (Simple) auf dem zweiten Laufwerk wiederhergestellt.

Recovery auf ein noch nicht initialisiertes Laufwerk

In diesem Fall wird das Ziellaufwerk automatisch mit dem Partitionsschema MBR initialisiert. Die dynamischen Volumes werden als Volumes vom Typ 'Basis' wiederherstellt. Falls die Volumes auf den 'nicht zugeordneten' Speicherplatz nicht passen sollten, wird ihre Größe proportional angepasst (durch Verringerung ihres freien Speicherplatzes).

Die untere Tabelle demonstriert die resultierenden Volume-Typen, abhängig von Backup-Quelle und Recovery-Ziel.

	Backup (Quelle):	
Wiederhergestellt zu:	**Dynamisches Volume**	**Basis-Volume**
Dynamisches Volume	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Typ wie der des Ziels
Nicht zugeordneter Speicherplatz (Laufwerksgruppe)	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Einfach
Basis-Volume oder 'nicht zugeordneter' Speicherplatz auf einem Basis-Laufwerk	Basis-Volume	Basis-Volume

Laufwerke während einer Wiederherstellung verschieben und in der Größe anpassen

Sie können das resultierende Basis-Volume während der Wiederherstellung manuell in der Größe anpassen oder seine Position auf dem Laufwerk ändern. Ein resultierendes dynamisches Volume kann nicht manuell verschoben oder in seiner Größe angepasst werden.

Datenträgergruppen und Laufwerke vorbereiten

Vor Wiederherstellung eines dynamischen Volumes auf ein fabrikneues System sollten Sie auf der Ziel-Hardware eine Laufwerksgruppe erstellen.

Möglicherweise müssen Sie auch verfügbaren, nicht zugeordneten Speicherplatz auf einer existierenden Laufwerksgruppe erstellen oder vergrößern. Dies kann durch Löschen von Laufwerken oder Konvertieren von Basis- zu dynamischen Datenträgern umgesetzt werden.

Möglicherweise wollen Sie den Typ des Ziel-Volumes ändern (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID 5). Dies kann durch Löschen des Ziellaufwerks und Erstellung eines neuen Laufwerks auf dem resultierenden 'nicht zugeordneten' Speicherplatz durchgeführt werden.

Acronis Backup enthält ein nützliches Disk Management Utility, welches Ihnen die Durchführung der oberen Aktionen ermöglicht (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director Lite siehe den Abschnitt Laufwerksverwaltung (S. 204).

3.8 Unterstützung für Festplatten mit Advanced Format (4K-Sektoren)

Acronis Backup kann sowohl Backups von Festplatten mit einer Sektorgröße von 4 KB erstellen (auch bekannt als Advanced Format-Laufwerke), wie auch von herkömmlichen Festplatten, die 512-Byte-Sektoren haben.

Acronis Backup kann Daten von einem dieser Laufwerke zu einem anderen wiederherstellen, solange *beide Laufwerke dieselbe logische Sektorgröße haben*. (Dies ist die gegenüber dem Betriebssystem präsentierte Sektorgröße.) Acronis Backup führt automatisch ein Alignment der Laufwerks-Volumes (S. 125) aus, sofern dies erforderlich ist. Auf diese Weise stimmt der Start eines Clusters im Dateisystem immer mit dem Start eines physikalischen Sektors auf dem Laufwerk überein.

Die Funktionalität zur Laufwerksverwaltungs (S. 204) von Acronis Backup steht für Laufwerke mit einer logischen Sektorgröße von 4-KB nicht zur Verfügung.

Bestimmung der logischen Sektorgröße

Anhand der Laufwerksspezifikation

Die Entwicklung der Advanced Format-Technologie wird von der 'International Disk Drive Equipment and Materials Association' (IDEMA) koordiniert. Weitere Details finden Sie unter http://www.idema.org/?page_id=2.

In Bezug auf die logische Sektorgröße spezifiziert die IDEMA zwei Typen von Advanced Format-Laufwerken:

- Laufwerke mit **512 Byte-Emulation (512e)** haben eine logische Sektorgröße von 512 Byte. Diese Laufwerke werden von Windows beginnend mit Windows Vista und von modernen Linux-Distributionen unterstützt. Microsoft und Western Digital verwenden den Ausdruck 'Advanced Format' exklusiv nur für diesen Laufwerkstyp.
- Laufwerke vom Typ **4K nativ (4Kn)** haben eine logische Sektorgröße von 4-KByte. Moderne Betriebssystem können Daten auf solchen Laufwerken speichern, meistens aber nicht von ihnen booten. Solche Laufwerken sind üblicherweise externe Laufwerke mit USB-Verbindung.

Durch Ausführung eines entsprechenden Befehls

Gehen Sie folgendermaßen vor, um die logische Sektorgröße eines Laufwerks zu ermitteln.

1. Stellen Sie sicher, dass das Laufwerk ein NTFS-Volume enthält.
2. Führen Sie folgenden Befehl als Administrator aus, unter Angabe des Laufwerksbuchstaben für das NTFS-Volume:

```
fsutil fsinfo ntfsinfo D:
```

3. Bestimmen Sie den Wert in der Zeile **Bytes pro Sektor**. Die Ausgabe kann beispielsweise wie folgt aussehen:

```
Bytes Per Sector : 512
```

3.9 Kompatibilität mit Verschlüsselungssoftware

Acronis Backup behält seine komplette Funktionalität, wenn Sie es zusammen mit Verschlüsselungssoftware auf Dateiebene einsetzen.

Verschlüsselungssoftware auf Laufwerksebene verschlüsselt Daten 'on the fly'. Daher sind die entsprechenden, in ein Backup aufgenommenen Daten nicht verschlüsselt. Programme zur Laufwerksverschlüsselung modifizieren häufig wichtige Systembereiche: Boot-Record oder Partitionstabellen oder Dateisystemtabellen. Diese Faktoren haben einen Einfluss auf Backup- und Recovery-Aktionen auf Laufwerksebene sowie auf die Fähigkeit eines wiederhergestellten Systems, zu booten oder auf die Acronis Secure Zone zuzugreifen.

Unter bestimmten Bedingungen ist Acronis Backup jedoch mit folgenden Programmen zur Laufwerksverschlüsselung kompatibel:

- Microsoft BitLocker-Laufwerksverschlüsselung
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

Um zuverlässige Wiederherstellungen auf Laufwerksebene zu garantieren, sollten Sie entsprechenden allgemeinen Regeln sowie den Software-spezifischen Empfehlungen folgen.

Allgemeine Installationsregel

Es wird dringend empfohlen, eine Verschlüsselungssoftware vor der Installation von Acronis Backup einzurichten.

Verwendung der Acronis Secure Zone

Eine Acronis Secure Zone darf keiner Laufwerksverschlüsselung unterzogen werden. Das ist einzige Art, die Acronis Secure Zone dann zu verwenden:

1. Installieren Sie zuerst die Verschlüsselungssoftware und dann Acronis Backup.
2. Erstellen Sie eine Acronis Secure Zone
3. Schließen Sie die Acronis Secure Zone von der Verschlüsselung des Laufwerks oder seiner Volumes aus.

Allgemeine Backup-Regel

Sie können ein Laufwerk-Backup im Betriebssystem durchführen. Versuchen Sie nicht, das Backup unter Verwendung eines bootfähigen Mediums oder des Acronis Startup Recovery Manager durchzuführen.

Software-spezifische Recovery-Prozeduren

Microsoft BitLocker-Laufwerksverschlüsselung

So stellen Sie ein System wieder her, das per BitLocker verschlüsselt wurde:

1. Booten Sie mit einem bootfähigen Medium.
2. Stellen Sie das System wieder her. Die wiederhergestellten Daten sind unverschlüsselt.

3. Booten Sie das wiederhergestellte System neu.
4. Schalten Sie die BitLocker-Funktion ein.

Falls Sie nur ein Volume eines mehrfach partitionierten Laufwerks wiederherstellen müssen, so tun Sie dies unter dem Betriebssystem. Eine Wiederherstellung mit einem bootfähigen Medium kann dazu führen, dass das wiederhergestellte Volume (die Partition) für Windows nicht mehr erkennbar ist.

McAfee Endpoint Encryption und PGP Whole Disk Encryption

Sie können ein verschlüsseltes System-Volume nur durch Verwendung eines bootfähigen Mediums wiederherstellen.

Falls das wiederhergestellte System nicht mehr bootet, erstellen Sie einen neuen Master Boot Record, wie in folgendem Artikel der Acronis Knowledge Base beschrieben: http://kb.acronis.com/content/1507 und booten Sie dann neu.

3.10 Unterstützung für SNMP

SNMP-Objekte

Acronis Backup stellt die folgenden Simple Network Management Protocol (SNMP)-Objekte für SNMP-Verwaltungsanwendungen zur Verfügung:

- Typ des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Syntax: OctetString

  Der Wert kann „Information“, „Warnung“, „Fehler“ und „Unbekannt“ sein. „Unbekannt“ wird nur in der Testnachricht gesendet.
- Textbeschreibung des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Syntax: OctetString

  Der Wert enthält die Textbeschreibung des Ereignisses (identische Darstellung wie in den Meldungen der Ereignisanzeige von Acronis Backup).

Beispiele für Varbind-Werte:

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Unterstützte Aktionen

Acronis Backup **unterstützt nur TRAP-Aktionen**. Es ist nicht möglich, Acronis Backup unter Verwendung von GET- und SET-Anforderungen zu verwalten. Das bedeutet, dass Sie einen SNMP-TRAP-Receiver verwenden müssen, um TRAP-Meldungen zu empfangen.

Über die Management Information Base (MIB)

Die MIB-Datei **acronis-abr.mib** befindet sich im Installationsverzeichnis von Acronis Backup. Standardmäßig: %ProgramFiles%\Acronis\BackupAndRecovery unter Windows und /usr/lib/Acronis/BackupAndRecovery unter Linux.

Diese Datei kann von einem MIB-Browser oder einem einfachen Texteditor (wie Notepad oder vi) gelesen werden.

Über die Testnachricht

Sie können bei der Konfiguration von SNMP-Benachrichtigungen eine Testnachricht versenden, um zu überprüfen, ob Ihre Einstellungen richtig sind.

Die Parameter der Testnachricht lauten folgendermaßen:

- Typ des Ereignisses
  OID: 1.3.6.1.4.1.24769.100.200.1.0
  Wert: „Unbekannt“
- Textbeschreibung des Ereignisses
  OID: 1.3.6.1.4.1.24769.100.200.2.0
  Wert: "?00000000"

3.11 Unterstützung für Windows 8 und Windows Server 2012

Dieser Abschnitt beschreibt, wie Acronis Backup Funktionen unterstützt, die mit den Windows 8- und Windows Server 2012-Betriebssystemen eingeführt wurden.

Die Informationen in diesem Abschnitt gelten außerdem für Windows 8.1 und den Windows Server 2012 R2.

Beschränkungen

- Der Acronis Disk Director Lite (S. 204) ist unter Windows 8 und dem Windows Server 2012 nicht verfügbar.
- Aktionen zur Laufwerksverwaltung funktionieren unter einem bootfähigen Medium möglicherweise nicht korrekt, falls auf der Maschine Speicherplätze (Storage Spaces) konfiguriert sind.
- Die Windows To Go-Funktion von Windows 8 wird nicht unterstützt.

WinPE 4.0 und WinPE 5.0

Der Acronis Media Builder kann bootfähige Medien erstellen, die auf diesen Versionen von Windows Preinstallation Environment (WinPE) basieren.

Diese bootfähigen Medien unterstützen neue Funktionen von Windows 8 und dem Windows Server 2012 (siehe weiter unten in diesem Abschnitt). Sie können auf bzw. mit Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.

Sie benötigen zur Erstellung von bootfähigen Medien, die auf diesen WinPE-Versionen basieren, das Windows Assessment and Deployment Kit (ADK) Weitere Details finden Sie im Abschnitt 'WinPE-basierte bootfähige Medien (S. 195)'.

UEFI Secure Boot

Auf einer unter Windows 8 oder Windows Server 2012 laufenden Maschine, die UEFI verwendet, kann die UEFI-Funktion 'Secure Boot' (auch 'Sicherer Start' genannt) angeschaltet sein. Secure Boot gewährleistet, dass die Maschine nur von vertrauenswürdigen Boot-Loadern gestartet werden kann.

Durch Verwendung des Acronis Media Builder können Sie ein bootfähiges Medium erstellen, das über einen vertrauenswürdigen Boot-Loader verfügt. Wählen Sie dazu, dass ein Linux-basiertes 64-Bit-Medium oder ein auf WinPE 4 (oder höher) basierendes 64-Bit-Medium erstellt werden soll.

Robustes Dateisystem (Resilient File System, ReFS)

Sie können in Windows Server 2012 ein Volume mit dem ReFS-Dateisystem formatieren. Dieses Dateisystem bietet im Vergleich zum NTFS-Dateisystem zuverlässigere Verfahren beim Speichern von Daten auf Volumes.

Sie können unter dem **Windows Server 2012** und unter einem **auf WinPE 4 (oder höher) basierenden bootfähigen Medium** ein ReFS-Volume per Backup sichern und wiederherstellen. Eine Größenanpassung von ReFS-Volumes während einer Wiederherstellung wird nicht unterstützt.

Linux-basierte bootfähige Medien und bootfähige Medien, die auf **WinPE vor Version 4.0** basieren, können keine Dateien auf ReFS-Volumes schreiben. Sie können mit solchen Medien daher auch keine Dateien zu einem ReFS-Volume wiederherstellen und ein ReFS-Volume auch nicht als Backup-Ziel auswählen.

Speicherplätze (Storage Spaces)

Unter Windows 8 und Windows Server 2012 ist es möglich, mehrere physikalische Laufwerke zu einem *Speicherpool* (Storage Pool) zu kombinieren. In diesem Speicherpool können wiederum ein oder mehrere logische Datenträger (Disks) erstellt werden, die Speicherplätze (Storage Spaces) genannt werden. Speicherplätze können wie gewöhnliche Laufwerke ebenfalls Volumes haben.

Sie können unter **Windows 8**, unter dem **Windows Server 2012** und unter einem **auf WinPE 4 (oder höher) basierenden Boot-Medium** Backup- und Recovery-Aktionen mit Speicherplätzen durchführen. Unter dem Windows Server 2012 und unter einem auf WinPE 4 (oder höher) basierenden Boot-Medium können Sie außerdem einen Speicherplatz (Storage Space) zu einem herkömmlichen Laufwerk wiederherstellen (und umgekehrt).

Linux-basierte Boot-Medien können keine Speicherplätze erkennen. Sie sichern die zugrundeliegenden Laufwerke aber per Sektor-für-Sektor-Backup. Falls Sie alle zugrundeliegenden Laufwerke zu den *ursprünglichen* Laufwerken wiederherstellen, werden auch die Speicherplätze (Storage Spaces) wieder neu erstellt.

Datendeduplizierung

Unter Windows Server 2012 können Sie die Datendeduplizierungsfunktion für NTFS-Volumes aktivieren. Datendeduplizierung reduziert den auf dem Volume belegten Speicherplatz, indem doppelt vorhandene Fragemente der Dateien des Volumes nur je einmal gespeichert werden.

Sie können ein Volume, für das die Datendeduplizierung aktiviert ist, auf Laufwerksebene ohne Einschränkungen per Backup sichern und wiederherstellen. Backups auf Dateiebene und Datei-Recovery (einschließlich Datei-Recovery von Laufwerk-Backups) werden nicht unterstützt.

3.12 Unterstützung für UEFI-basierte Maschinen

Acronis Backup kann Maschinen, die 64-Bit-UEFI (Unified Extensible Firmware Interface) verwenden, auf die gleiche Art sichern und wiederherstellen, wie es für Maschinen der Fall ist, die BIOS zum Booten verwenden.

Das gilt für physikalische und virtuelle Maschinen; und auch unabhängig davon, ob die virtuellen Maschinen auf Hypervisor-Ebene oder innerhalb eines Gast-Betriebssystems gesichert werden.

Backup und Recovery von Geräten, die 32-Bit-UEFI verwenden, wird nicht unterstützt.

Weitere Details zum Überführen von Windows-Maschinen zwischen UEFI und BIOS finden Sie im Abschnitt 'Recovery von BIOS-basierten Systemen zu UEFI-basierten Systemen und umgekehrt (S. 131)'.

Beschränkungen

- Auf WinPE-basierende Boot-Medien mit einer Version früher als 4.0 unterstützen kein Booten per UEFI.
- Acronis Active Restore (S. 293) steht auf UEFI-Maschinen nicht zur Verfügung.
- Der Acronis Startup Recovery Manager (ASRM) (S. 293) kann auf UEFI-Maschinen nur unter Windows aktiviert werden.

4 Backup

4.1 Backup jetzt

Verwenden Sie die Funktion **Backup jetzt**, um ein einmaliges Backup mit wenigen einfachen Schritten zu konfigurieren und zu starten. Der Backup-Prozess wird unmittelbar ausgeführt, sobald Sie alle benötigten Schritte durchgeführt und auf **OK** geklickt haben.

Für längerfristige Backup-Strategien, die Planung und Bedingungen einschließen (etwa zeitbedingtes Löschen oder Verschieben von Backups zu anderen Speicherorten), sollten Sie besser die Erstellung eines Backup-Plans erwägen.

Die Konfiguration eines sofortigen Backups gleicht der Erstellung eines Backup-Plans (S. 38) mit folgenden Unterschieden:

- Es gibt keine Optionen zur Planung von Backups oder zur Konfiguration von Aufbewahrungsregeln.
- Eine vereinfachte Benennung der Backup-Dateien (S. 61) wird verwendet, sofern dies vom Backup-Ziel unterstützt wird. Anderenfalls wird die Standard-Backup-Benennung verwendet.

  Folgende Speicherorte unterstützen keine vereinfachte Dateibenennung: Bänder, die Acronis Secure Zone oder der Acronis Cloud Storage.

  Aufgrund der vereinfachten Dateibenennung kann ein RDX- oder USB-Flash-Laufwerk nur im Modus Wechselmedium (S. 170) verwendet werden.
- Die Möglichkeit zum Konvertieren eines Laufwerk-Backups zu einer virtuellen Maschine steht nicht als Teil der Backup-Aktion zur Verfügung. Sie können die resultierenden Backups aber anschließend konvertieren.

4.2 Erstellung eines Backup-Plans

Bevor Sie Ihren ersten Backup-Plan (S. 295) erstellen, sollten Sie sich mit den grundlegenden Konzepten vertraut machen, die in Acronis Backup verwendet werden.

Zur Erstellung eines Backup-Plans führen Sie folgende Schritte aus.

Backup-Quelle

Elemente für das Backup (S. 41)

Wählen Sie den zu sichernden Datentyp und spezifizieren Sie die Datenelemente für das Backup. Der Typ der Daten hängt von den auf der Maschine installierten Agenten ab.

Anmeldedaten, Ausschließungen

Klicken Sie auf **Anmeldedaten, Ausschließungen anzeigen**, um auf diese Einstellung zugreifen zu können.

Anmeldedaten (S. 41)

Stellen Sie Anmeldedaten für die Quelldaten zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für die Daten hat.

Ausschließungen (S. 42)

Definieren Sie Ausschließungen für spezifische Datei-Typen, die Sie nicht mit ins Backup aufnehmen wollen.

Backup-Ziel

Speicherort (S. 44)

Spezifizieren Sie einen Pfad zu dem Ort, wo das Backup-Archiv gespeichert wird, sowie den Namen des Archivs. Der Archivname muss innerhalb des Zielordners eindeutig sein. Anderenfalls werden die Backups des neu erstellten Backup-Plans bei einem bereits existierenden Archiv hinterlegt, das zu einem anderen Backup-Plan gehört. Der vorgegebene Archivname ist Archive(N), wobei N die fortlaufende Nummer des Archivs im gewählten Speicherort ist.

Wählen Sie den Modus, in dem das Wechsellaufwerk verwendet wird (S. 170)

Sollte es sich beim angegebenen Speicherort um ein RDX- oder USB-Flash-Laufwerk handeln, dann wählen Sie den Gerätemodus: **Wechselmedium** oder **Eingebautes Laufwerk**.

Benennung der Backup-Datei, Anmeldedaten, Archivkommentare

Klicken Sie auf **Benennung der Backup-Datei, Anmeldedaten, Archivkommentare anzeigen**, um Zugriff auf diese Einstellungen zu erhalten.

Dateibenennung (S. 61)

[Optional] Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen, wie in Acronis True Image Echo, anstelle automatisch generierter Namen**, falls Sie für die Backups des Archivs eine vereinfachte Dateibenennung verwenden wollen.

Nicht verfügbar, wenn Sie Backups zu einem verwalteten Depot, auf ein Band, in die Acronis Secure Zone oder in den Acronis Cloud Storage durchführen. Beim Backup zu einem RDX- oder USB-Flash-Laufwerk wird das Dateibenennungsschema durch den Wechsellaufwerkmodus (S. 170) *bestimmt.*

Anmeldedaten (S. 46)

[Optional] Stellen Sie Anmeldedaten für den Speicherort zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für den Ort hat.

Archiv-Kommentare

[Optional] Tragen Sie Kommentare für das Archiv ein.

Single-Pass-Laufwerk- und Anwendungs-Backup

Gilt nur für Maschinen, die über eine Lizenz für Single-Pass-Backup verfügen.

Spezifizieren Sie für Single-Pass-Laufwerk- und Anwendungs-Backups geltende Einstellungen.

Art des Backups

Backup-Schema (S. 47)

Spezifizieren Sie, wann und wie oft Ihre Daten gesichert werden sollen, definieren Sie, wie lange die erzeugten Backup-Archive im gewählten Speicherort aufbewahrt werden sollen; erstellen Sie einen Zeitplan zur Bereinigung der Archive (siehe den nachfolgenden Abschnitt 'Replikations- und Aufbewahrungseinstellungen').

Replikations- und Aufbewahrungseinstellungen (S. 79)

Nicht verfügbar für Wechselmedien oder wenn die vereinfachte Benennung für Backup-Dateien (S. 61) *gewählt wurde.*

Definieren Sie, ob die Backups zu einem anderen Speicherort kopiert (repliziert) werden sollen – und ob sie gemäß den Aufbewahrungsregeln verschoben oder gelöscht werden sollen. Die verfügbaren Einstellungen hängen vom Backup-Schema ab.

2. Speicherort

[Optional] Aktivieren Sie zur Einrichtung einer Backup-Replikation das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren**. Zu weiteren Informationen über Backup-Replikation siehe 'Replikation von Backups einrichten (S. 81)'.

Validierung, zu virtueller Maschine konvertieren

Klicken Sie auf **Anzeigen: Validierung, zu virtueller Maschine konvertieren**, um Zugriff auf diese Einstellungen zu erhalten.

Validierungszeitpunkt (S. 57)

[Optional] Definieren Sie, abhängig vom gewählten Backup-Schema, wann und wie oft eine Validierung durchzuführen ist und ob das komplette Archiv oder nur das letzte Backup im Archiv validiert werden soll.

Zu virtueller Maschine konvertieren (S. 153)

[Optional] Gilt für: Laufwerk/Volume-Backups, die Backups kompletter virtueller Maschinen oder die Volumes einer virtuellen Maschine.

Richten Sie die regelmäßige Konvertierung eines Laufwerk- oder Volume-Backups zu einer virtuellen Maschine ein.

Plan-Parameter

Plan-Name

[Optional] Geben Sie einen eindeutigen Namen für den Backup-Plan ein. Ein bewusst gewählter Name macht es leichter, diesen Plan zu identifizieren.

Backup-Optionen

[Optional] Konfigurieren Sie Parameter für eine Backup-Aktion, wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt wird, oder den Komprimierungsgrad für das Backup-Archiv. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 87) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert in einer Zeile angezeigt. Der Einstellungsstatus ändert sich von **Standard** zu **Auf Standard zurücksetzen**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Wenn der Standardwert eingestellt wird, verschwindet die Zeile. Sie sehen daher in diesem Abschnitt immer nur die Einstellungen, die von den Standardwerten abweichen.

Um alle Einstellungen auf Standardwerte zurückzusetzen, klicken Sie auf **Auf Standard zurücksetzen**.

Anmeldedaten des Plans, Kommentare, Bezeichnung

Klicken Sie auf **Anmeldedaten des Plans, Kommentare, Bezeichnung anzeigen**, um auf diese Einstellung zugreifen zu können.

Anmeldedaten des Plans (S. 58)

[Optional] Spezifizieren Sie die Anmeldedaten, unter denen der Plan laufen soll.

Kommentare

[Optional] Geben Sie eine Beschreibung bzw. einen Kommentar für den Backup-Plan ein.

Bezeichnung (S. 58)

[Optional] Geben Sie für die zu sichernde Maschine eine Textbezeichnung ein. Diese Bezeichnung kann verwendet werden, um die Maschine in verschiedenen Szenarien zu identifizieren.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Backup-Plan zu erstellen.

Danach kann es sein, dass Sie zur Eingabe eines Kennworts (S. 61) aufgefordert werden.

Sie können auf den von Ihnen erstellten Plan in der Ansicht **Backup-Pläne und Tasks** (S. 249) zur Untersuchung und Verwaltung zugreifen.

4.2.1 Daten für ein Backup auswählen

So wählen Sie Daten für ein Backup aus

1. Bestimmen Sie im Abschnitt **Daten für das Backup** den Typ derjenigen Daten, die Sie sichern wollen. Die Liste der verfügbaren Datentypen hängt von den Agenten ab, die auf der Maschine laufen und den Lizenztypen:

   Laufwerke/Volumes

   Ist verfügbar, wenn der Acronis Backup Agent für Windows oder der Acronis Backup Agent für Linux installiert ist.

   Wählen Sie diese Option, um komplette physikalische Maschinen oder einzelne Laufwerke bzw. Volumes von diesen zu sichern. Sie müssen Benutzerrechte als Administrator oder Sicherungs-Operator haben, um diese Daten sichern zu können.

   Ein Laufwerk-Backup ermöglicht Ihnen, ein komplettes System auch bei schwerer Datenbeschädigung oder Hardware-Ausfall wiederherzustellen. Sie können außerdem einzelne Dateien und Ordner wiederherstellen. Diese Backup-Prozedur ist schneller als ein einfaches Kopieren von Dateien und kann Backup-Prozesse beim Sichern großer Datenmengen signifikant beschleunigen.

   Ordner/Dateien

   Ist verfügbar, wenn der Acronis Backup Agent für Windows oder der Acronis Backup Agent für Linux installiert ist.

   Aktivieren Sie diese Option, um spezifische Dateien und Ordner zu sichern.

   Ein dateibasiertes Backup ist zur Wiederherstellung eines Betriebssystems nicht ausreichend geeignet. Verwenden Sie ein Datei-Backup, wenn Sie nur bestimmte Daten (beispielsweise ein aktuelles Projekt) sicher bewahren wollen. Das reduziert die Archivgröße und spart so Speicherplatz.

   Um Ihr Betriebssystem mit all seinen Einstellungen und Anwendungsprogrammen wiederherstellen zu können, müssen Sie ein Laufwerk-Backup durchführen.

2. Bestimmen Sie im Verzeichnisbaum unterhalb des Abschnittes **Daten für das Backup** die zu sichernden Elemente, indem Sie die neben diesen liegenden Kontrollkästchen aktivieren.

   Um alle auf einer Maschine präsenten Elemente des gewählten Datentyps zu sichern, aktivieren Sie das Kontrollkästchen neben der Maschine. Um einzelne Datenelemente zu sichern, müssen Sie die Maschine erweitern und die Kontrollkästchen neben den gewünschten Elementen aktivieren.

   Hinweis für Laufwerke/Volumes

   - Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht mehr startet.

3. Klicken Sie auf **OK**, wenn Sie die Daten für das Backup spezifiziert haben.

4.2.2 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, um auf die zu sichernden Daten zugreifen zu können.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Plans verwenden**

     Das Programm greift auf die Quelldaten mit den Anmeldedaten des Backup-Plan-Kontos zu, wie sie im Abschnitt **Plan-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu.

     Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffserlaubnis für die Daten hat.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

4.2.3 Ausschluss von Quelldateien

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist nur für Backups auf *Laufwerksebene* von NTFS-, FAT-, Ext3- und Ext4-Dateisystemen wirksam. Diese Option ist bei Backups auf *Dateiebene* für alle unterstützten Dateisysteme wirksam.

Diese Option definiert, welche Dateien und Ordner während des Backup-Prozesses übersprungen und so von der Liste der zu sichernden Elemente ausgeschlossen werden.

Hinweis: *Ausschließungen überschreiben eine Auswahl von Datenelementen, die per Backup gesichert werden sollen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' per Backup gesichert werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht mitgesichert.*

Setzen Sie folgende Parameter, um die auszuschließenden Dateien und Ordner zu spezifizieren.

Alle versteckten Dateien und Ordner ausschließen

Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, die mit dem Attribut **Versteckt** gekennzeichnet sind (bei von Windows unterstützten Dateisystemen) – oder die mit einem Punkt (.) beginnen (bei Dateisystemen unter Linux wie Ext2 und Ext3). Bei Ordnern mit dem Attribut 'Versteckt' wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht versteckt sind).

Ausschluss aller Systemdateien und -ordner

Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **System** zu überspringen. Bei Ordnern mit dem Attribut **System** wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht mit dem Attribut **System** gekennzeichnet sind).

Tipp: *Sie können die Attribute von Dateien oder Ordnern über ihre Datei-/Ordner-Eigenschaften einsehen -– oder mit dem Kommandozeilenbefehl* ***attrib****. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

Dateien ausschließen, die folgende Kriterien erfüllen

Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner zu überspringen, die einem der Kriterien entsprechen. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Kriterien zu verwalten.

Bei den Kriterien wird *nicht* auf Groß-/Kleinschreibung geachtet (in Windows und Linux). Falls Sie beispielsweise festlegen, dass alle .tmp-Dateien und der Ordner C:\Temp ausgeschlossen werden sollen, dann werden auch alle .Tmp-Dateien, alle .TMP-Dateien und der Ordner C:\TEMP ausgeschlossen.

Kriterium: vollständiger Pfad

Spezifizieren Sie den vollständigen Pfad zu der Datei oder dem Ordner, indem Sie mit dem Laufwerksbuchstaben (bei Backups unter Windows) oder dem Stammverzeichnis (bei Backups unter Linux) beginnen.

Sie können unter Windows und Linux im Datei- bzw. Ordnerpfad einen normalen Schrägstrich (Slash) verwenden (wie bei **C:/Temp** und **C:/Temp/Datei.tmp**). Unter Windows können Sie auch den üblichen, nach links geneigten Schrägstrich (Backslash) verwenden (wie bei **C:\Temp** und **C:\Temp\Datei.tmp**).

Beim Verwenden eines Windows-typischen bootfähigen Mediums kann ein Volume einen anderen Laufwerksbuchstaben als unter Windows haben. Weitere Informationen finden Sie im Abschnitt 'Mit bootfähigen Medien arbeiten (S. 199)'.

Kriterium: name

Spezifizieren Sie den Namen der Datei oder des Ordners, wie etwa 'Dokument.txt'. Alle Dateien und Ordner mit diesem Namen werden ausgeschlossen.

Platzhalterzeichen (Wildcards)

Sie können ein oder mehrere Platzhalterzeichen (* und ?) in dem Kriterium verwenden. Diese Zeichen können innerhalb des vollständigen Pfades und im Namen der Datei oder des Ordners verwendet werden.

Das Asterisk (*) ersetzt null bis mehrere Zeichen in einem Dateinamen. So beinhaltet beispielsweise das Kriterium 'Doc*.txt' Dateien wie 'Doc.txt' und 'Document.txt'.

Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen. Beispielsweise beinhaltet das Kriterium 'Doc?.txt' Dateien wie 'Doc1.txt' und 'Docs.txt' – aber nicht 'Doc.txt' oder 'Doc11.txt'.

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
		Windows und Linux
Per Name	F.log F	Schließt alle Dateien namens 'F.log' aus Schließt alle Ordner namens 'F' aus
Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)

Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen
Windows		
Per Dateipfad	C:\Finanzen\F.log	Schließt eine Datei aus, die 'F.log' heißt und im Ordner 'C:\Finanzen' vorliegt
Per Ordnerpfad	C:\Finanzen\F *oder* C:\Finanzen\F\	Schließt den Ordner 'C:\Finanzen\F' aus (stellen Sie sicher, dass Sie den vollständigen Pfad angeben, beginnend mit einem Laufwerksbuchstaben)
Linux		
Per Dateipfad	/home/user/Finanzen/F.log	Schließt eine Datei aus, die 'F.log' heißt und im Ordner (Verzeichnis) '/home/user/Finanzen' vorliegt
Per Ordnerpfad	/home/user/Finanzen *oder* /home/user/Finanzen/	Schließt den Ordner (Verzeichnis) '/home/user/Finanzen' aus

4.2.4 Auswahl der Backup-Speicherortes

Spezifizieren Sie, wo das Archiv gespeichert werden soll.

1. Ziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel aus dem Verzeichnisbaum (wie im Abschnitt 'Auswahl der Backup-Zielorte (S. 45)' beschrieben.

2. Archiv-Tabelle verwenden

Die Tabelle zeigt für jeden gewählten Speicherort die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Sobald Sie den Zielort für das Archiv gewählt haben, erstellt das Programm einen Namen für das neue Archiv und zeigt diesen im Feld **Name** an. Der Name sieht üblicherweise aus wie *Archiv(N)*, wobei *N* eine fortlaufende Nummer ist. Der generierte Name ist innerhalb des gewählten Speicherortes eindeutig. Wenn Sie mit dem automatisch generierten Namen einverstanden sind, dann klicken Sie auf **OK**. Geben Sie anderenfalls einen eindeutigen Namen ein.

Backup zu einem existierenden Archiv

Sie können einen Backup-Plan so konfigurieren, dass das Backup zu einem existierenden Archiv erfolgt. Zur Umsetzung wählen Sie das Archiv in der Tabelle oder geben die entsprechende Bezeichnung in das Feld **Name** ein. Sollte das Archiv mit einem Kennwort geschützt sein, wird das Programm in einem Pop-up-Fenster danach fragen.

Durch Wahl des existierenden Archivs erzeugen Sie eine Interaktion mit einem anderen Backup-Plan, der das Archiv ebenfalls verwendet. Das ist kein Problem, falls der andere unterbrochen wurde. Sie sollten im Allgemeinen jedoch folgender Regel folgen: „Ein Backup-Plan – ein Archiv“. Das Gegenteil zu tun, behindert das Programm nicht in seiner Funktion, ist aber unpraktisch bzw. uneffizient, mit Ausnahme einiger Spezialfälle.

Warum zwei oder mehr Backup-Pläne nicht in dasselbe Archiv sichern sollten

1. Wenn Sie unterschiedliche Quellen per Backup in dasselbe Archiv sichern, führt das zu schwierig handhabbaren Archiven. Wenn es darauf ankommt, eine wichtige Wiederherstellung durchzuführen, zählt jede Sekunde; Sie könnten sich in so einer Situation leicht im Inhalt des Archivs 'verlieren'.

   Mit demselben Archiv arbeitende Backup-Pläne sollten auch dieselben Daten-Elemente sichern (z.B. zwei Pläne, die Laufwerk C: sichern).

2. Werden auf ein Archiv multiple Aufbewahrungsregeln angewendet, so macht dies den Inhalt des Archivs unkalkulierbar. Da jede Regel auf das gesamte Archiv angewendet wird, kann es leicht passieren, dass Backups, die zu einem Backup-Plan gehören, zusammen mit Backups gelöscht werden, die zu einem anderen Plan gehören. Sie sollten kein klassisches Verhalten der Backup-Schemata GVS und Türme von Hanoi erwarten.

   Normalerweise sollte jeder komplexe Backup-Plan in 'eigene' Archive sichern.

4.2.4.1 Auswahl der Backup-Zielorte

Acronis Backup ermöglicht Ihnen, Backups zu verschiedenen physikalischen Speicherorten/-geräten (Storages) zu sichern.

Ziel	Details
Cloud Storage	Um Daten per Backup im bzw. zum Acronis Cloud Storage sichern zu können, klicken Sie auf **Anmelden** und geben Sie dann die Anmeldedaten ein, um sich am Cloud Storage anzumelden. Erweitern Sie dann die Gruppe **Cloud Storage** und wählen Sie das Konto. Bevor Sie Ihre Backups im bzw. zum Cloud Storage sichern können, müssen Sie für den Cloud Backup Service ein Abonnement kaufen (S. 285) und das Abonnement auf der zu sichernden Maschine aktivieren (S. 287). Cloud Backup steht unter bootfähigen Medien nicht zur Verfügung. ***Hinweis*** *Acronis Cloud Backup ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/cloud-backup/corporate*
Persönlich	Um Daten zu einem persönlichen Depot sichern zu können, erweitern Sie die Gruppe **Depots** und klicken auf das Depot. Die Acronis Secure Zone wird als persönliches Depot betrachtet, das für alle Benutzer verfügbar ist, die sich an diesem System anmelden können.
Maschine	Lokale Maschine
Lokale Ordner	Um Daten zu einem lokalen Ordner einer Maschine sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und dann den gewünschten Ordner auswählen.
CD, DVD, BD	Um Daten auf optische Medien wie CDs, DVDs oder Blu-ray-Medien (BD) sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und das gewünschte Laufwerk auswählen.
RDX, USB	Um Daten auf RDX- oder USB-Flash-Laufwerke sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und das gewünschte Laufwerk auswählen. Weitere Informationen über die Verwendung dieser Laufwerke finden Sie im Abschnitt 'Wechsellaufwerke (S. 170)'.
Bandgerät	Um Daten zu einem lokal angeschlossenen Bandgerät sichern zu können, erweitern Sie die Gruppe **<Maschinename>** und klicken dann auf das gewünschte Gerät. Bandgeräte stehen nur dann zur Verfügung, falls Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgeräte' in der Produkthilfe.

Ziel	Details
Netzwerkordner	Um Daten zu einem Netzwerkordner sichern zu können, müssen Sie die Gruppe **Netzwerkordner** erweitern, die gewünschte Netzwerkmaschine auswählen und dann auf den freigegebenen Ordner klicken. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
FTP, SFTP	Für Daten über FTP oder SFTP sichern zu können, geben Sie den Namen oder die Adresse des entsprechenden Servers wie folgt in das Feld **Pfad** ein: **ftp://ftp-server:port-nummer** oder **sftp://sftp-server:port-nummer** Verwenden Sie folgende Schreibweise, um eine FTP-Verbindung im aktiven Modus aufzubauen: **aftp://ftp-server:port-nummer** Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP. Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server. Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten. ***Anmerkung**: Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.*

4.2.5 Zugriff auf die Anmeldedaten für den Speicherort des Archivs

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Plans verwenden**

     Das Programm greift auf die Quelldaten mit den Anmeldedaten des Backup-Plan-Kontos zu, wie sie im Abschnitt **Plan-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu.

     Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffsberechtigungen für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

Warnung: *Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.*

4.2.6 Backup-Schemata

Wählen Sie eins der verfügbaren Backup-Schemata:

- **Einfach** – um zu planen, wann und wie oft die Daten gesichert werden und Aufbewahrungsregeln zu spezifizieren.
- **Großvater-Vater-Sohn** – um das Großvater-Vater-Sohn-Backup-Schema zu verwenden. Das Schema erlaubt es nicht, dass Daten mehr als einmal pro Tag gesichert werden. Sie bestimmen den Wochentag, an dem das tägliche Backup ausgeführt wird und wählen von diesen Tagen noch einen Tag zum wöchentlichen und monatlichen Backup. Dann definieren Sie die Aufbewahrungsregeln für die täglichen (entspricht dem „Sohn"), wöchentlichen („Vater") und monatlichen („Großvater") Backups. Abgelaufene Backups werden automatisch gelöscht.
- **Türme von Hanoi** – zur Verwendung des Backup-Schema 'Türme von Hanoi'. Mit diesem Schema können Sie planen, wann und wie oft Backups (Sitzungen) erfolgen sollen und eine entsprechende Zahl von Backup-Levels zu bestimmen (bis zu 16). Die Daten können dabei mehrmals pro Tag gesichert werden. Indem Sie die Backup-Planung aufstellen und die Backup-Level wählen, erhalten Sie automatisch die Roll-back-Periode – die garantierte Zahl von Sitzungen, zu der Sie jederzeit zurückgehen können. Der automatische Bereinigungsmechanismus hält die benötigte Roll-back-Periode aufrecht, indem er die abgelaufenen Backups löscht und von jedem Level die neusten Backups behält.
- **Benutzerdefiniert** – um ein benutzerdefiniertes Schema zu erstellen, das Ihnen ermöglicht, eine Backup-Strategie in der für Ihr Unternehmen benötigten Art aufzustellen: Spezifizieren Sie multiple Zeit-/Ereignis-Pläne für verschiedene Backup-Typen, fügen Sie Bedingungen hinzu und definieren Sie die Aufbewahrungsregeln.
- **Manueller Start** – um einen Backup-Task zum manuellen Start zu erstellen.
- **Initial Seeding** – zum lokalen Speichern eines Voll-Backups, welches später auf dem Acronis Cloud Storage hinterlegt wird.

4.2.6.1 Schema 'Einfach'

Mit dem Backup-Schema 'Einfach' planen Sie nur, wann und wie oft die Daten gesichert werden sollen. Andere Schritte sind optional.

Zur Einrichtung des Backup-Schemas 'Einfach' spezifizieren Sie die passenden Einstellungen wie folgt:

Planung

Legen Sie fest, wann und wie oft die Daten gesichert werden sollen. Siehe den Abschnitt Planung (S. 66), um mehr über das Einrichten von Zeit/-Ereignis-Planungen zu lernen.

Aufbewahrungsregeln

Spezifizieren Sie, wie lange Backups im Speicherort aufbewahrt werden sollen und ob sie danach verschoben oder gelöscht werden sollen. Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Standardmäßig ist die Option **Backups unbegrenzt behalten** aktiviert, was bedeutet, dass keine Backups automatisch gelöscht werden. Zu weiteren Informationen über Aufbewahrungsregeln siehe 'Aufbewahrungsregeln von Backups einstellen (S. 82)'.

Backup-Typ

Klicken Sie auf **Anzeigen: Backup-Typ, Validierung, zu virtueller Maschine konvertieren**, um Zugriff auf diese Einstellung zu erhalten.

Bestimmen Sie den Backup-Typ.

- **Vollständig** – Standardmäßig für alle Backup-Speicherorte (mit Ausnahme des Acronis Cloud Storages) vorausgewählt.
- **Inkrementell**. Beim ersten Mal wird immer ein Voll-Backup erstellt. Die nachfolgenden Backups werden inkrementell. Als einziger Backup-Typ für den Acronis Cloud Storage ausgewählt.

***Anmerkung**: Wenn der Backup-Typ **Inkrementell** zusammen mit den Aufbewahrungsregeln ausgewählt ist, erfolgt die Bereinigung des Archivs mit Hilfe der Konsolidierung (S. 301), was eine zeit- und ressourcenintensivere Aktion ist.*

4.2.6.2 Schema Großvater-Vater-Sohn

Auf einen Blick

- Tägliche ('Sohn'), wöchentliche ('Vater') und monatliche ('Großvater') Backups
- Benutzerdefinierbarer Tag für wöchentliche und monatliche Backups
- Benutzerdefinierbare Aufbewahrungsdauer für Backups jeden Typs

Beschreibung

Angenommen, Sie wollen einen Backup-Plan aufstellen, der regelmäßig eine Serie täglicher (T), wöchentlicher (W) und monatlicher (M) Backups produziert. Beispiel: Die nachfolgende Tabelle zeigt eine exemplarische zweimonatige Periode für einen solchen Plan.

	Mo	Di	Mi	Do	Fr	Sa	So
Jan 1—Jan 7	T	T	T	T	W	-	-
Jan 8—Jan 14	T	T	T	T	W	-	-
Jan 15—Jan 21	T	T	T	T	W	-	-
Jan 22—Jan 28	T	T	T	T	M	-	-
Jan 29—Feb 4	T	T	T	T	W	-	-
Feb 5—Feb 11	T	T	T	T	W	-	-
Feb 12—Feb 18	T	T	T	T	W	-	-
Feb 19—Feb 25	T	T	T	T	M	-	-
Feb 26—Mrz 4	T	T	T	T	W	-	-

Die täglichen Backups laufen an jedem Wochentag außer freitags, welcher für wöchentliche und monatliche Backups gelassen wird. Die monatlichen Backups laufen am letzten Freitag eines jeden Monats, während die wöchentlichen Backups an allen übrigen Freitagen laufen. Als Ergebnis erhalten Sie normalerweise 12 monatliche Backups über ein vollständiges Jahr hinweg.

Parameter

Sie können für ein Schema Großvater-Vater-Sohn (GVS) folgende Parameter einstellen.

Backup starten	Spezifiziert, wann das Backup starten soll. Der Standardwert ist 12:00 Uhr.
Backup auf	Spezifizieren Sie die Tage in der Woche, an denen ein Backup ausgeführt wird. Der Standardwert ist **Werktags**.

Wöchentlich/monatlich:	Spezifiziert, welchen Tag in der Woche (der im Feld **Backup an** gewählten Tage) Sie für wöchentliche und monatliche Backups reservieren wollen. Der Standardwert ist **Freitag**. Mit diesem Wert wird ein monatliches Backup am letzten Freitag eines jeden Monats ausgeführt. Wöchentliche Backups werden an allen anderen Freitagen ausgeführt. Sollten Sie einen anderen Tag der Woche wählen, dann werden diese Regeln auf den ausgewählten Tag angewendet.
Backups behalten	Spezifiziert, wie lange die Backups im Archiv gespeichert werden sollen. Die Zeitdauer kann in Stunden, Tagen, Wochen, Monaten oder Jahren gesetzt werden. Für monatliche Backups können Sie auch **Unbegrenzt behalten** wählen, falls Sie diese für immer speichern wollen. Die Standardwerte für jeden Backup-Typ sind wie folgt: Täglich: 5 Tage (empfohlenes Minimum) Wöchentlich: 7 Wochen Monatlich: unbegrenzt Die Aufbewahrungsdauer für wöchentliche Backups muss die für tägliche überschreiten; die Periode für monatliche Backups muss größer sein als die für wöchentliche. Es wird für tägliche Backups eine Aufbewahrungsdauer von wenigstens einer Woche empfohlen.
Backup-Typ	Spezifiziert den Typ der täglichen, wöchentlichen und monatlichen Backups. ▪ **Immer vollständig** – alle täglichen, wöchentlichen und monatlichen Backups sind immer vollständig. Das ist die Standardauswahl für Fälle, in denen ein Bandgerät als Backup-Speicherort ausgewählt wird. ▪ **Vollständig/Differentiell/Inkrementell** – tägliche Backups sind inkrementell, wöchentliche Backups differentiell und monatliche Backups sind vollständig. Das erste Backup ist immer vollständig. Dies bedeutet jedoch nicht, dass es ein monatliches Backup ist. Es wird als tägliches, wöchentliches oder monatliches Backup aufbewahrt, abhängig vom Wochentag, an dem es erstellt wurde.

Ein Backup wird solange nicht gelöscht, bis alle auf ihm beruhenden Backups ebenfalls von einer Löschung betroffen sind. Aus diesem Grund kann es sein, dass Sie ein Backup sehen (mit dem Symbol gekennzeichet), welches noch einige Tage über sein Ablaufdatum im Archiv verbleibt.

Beispiele

Jeder Tag der vergangenen Woche, jede Woche des vergangenen Monats

Betrachten wir ein allgemein als nützlich angesehenes GVS-Backup-Schema.

- Dateien jeden Tag sichern, einschließlich am Wochenende
- Ermöglicht die Wiederherstellung von Dateien von jedem der vergangenen sieben Tage
- Zugriff auf die wöchentlichen Backups des vergangenen Monats haben.
- Monatliche Backups unbegrenzt behalten.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **23:00:00 Uhr**
- Sichern: **Alle Tage**
- Wöchentlich/monatlich: **Samstag** (als Beispiel)
- Backups aufbewahren:

  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Als Ergebnis wird ein Archiv aus täglichen, wöchentlichen und monatlichen Backups erstellt. Tägliche Backups sind für die sieben Tage seit Erstellung verfügbar. Ein Beispiel: Ein tägliches Backup vom Sonntag (1. Januar) wird bis zum nächsten Sonntag (8. Januar) verfügbar sein, das erste wöchentliche Backup vom Samstag (7. Januar) wird auf dem System bis zum 7. Februar gespeichert. Monatliche Backups werden nie gelöscht.

Begrenzte Speicherung

Sofern Sie nicht eine Unmenge von Platz zur Speicherung eines riesigen Archivs einrichten wollen, sollten Sie ein GVS-Schema aufsetzen, welches Ihre Backups kurzlebiger macht, gleichzeitig aber auch sicherstellt, dass Ihre Informationen im Fall eines unbeabsichtigten Datenverlustes wiederhergestellt werden können.

Angenommen, Sie müssen:

- Backups am Ende eines jeden Arbeitstages durchführen
- fähig sein, eine versehentlich gelöschte oder ungewollt modifizierte Datei wiederherzustellen, falls dies relativ schnell entdeckt wurde
- zehn Tage nach seiner Erstellung noch Zugriff auf ein wöchentliches Backup haben
- monatliche Backups für ein halbes Jahr aufbewahren.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **18:00:00 Uhr**
- Sichern: **Werktags**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **10 Tage**
  - Monatlich: **6 Monate**

Mit Hilfe dieses Schemas steht Ihnen eine Woche zur Verfügung, um die frühere Version einer beschädigten Datei aus einem täglichen Backup wiederherzustellen, außerdem haben Sie einen 10-Tage-Zugriff auf wöchentliche Backups. Jedes monatliche Voll-Backup wird über sechs Monate nach seinem Erstelldatum verfügbar sein.

Arbeitsplan

Angenommen, Sie sind Finanzberater in Teilzeit und arbeiten dienstags und donnerstags in einer Firma. An diesen Tagen führen Sie häufig Änderungen an Ihren Finanzdokumenten, Mitteilungen durch und aktualisieren Ihre Tabellenkalkulationen etc. auf Ihrem Notebook. Um diese Daten per Backup zu sichern, wollen Sie vermutlich:

- die Veränderungen an den finanziellen Mitteilungen, Tabellenkalkulationen etc. verfolgen, die Sie dienstags und donnerstags durchgeführt haben (tägliches inkrementelles Backup).
- eine wöchtenliche Zusammenfassung aller Dateiveränderungen seit dem letzten Monat haben (wöchentliche differentielle Backups am Freitag)
- ein monatliches Voll-Backup Ihrer Dateien haben.

Weiterhin sei angenommen, dass Sie sich einen Zugriff auf alle Backups, inkl. der täglichen, für wenigstens sechs Monate bewahren wollen.

Das nachfolgende GVS-Schema passt für diesen Zweck:

- Backup starten: **23:30 Uhr**
- Sichern: **Dienstag, Donnerstag, Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **6 Monate**
  - Wöchentlich: **6 Monate**
  - Monatlich: **5 Jahre**

Tägliche inkrementelle Backups werden hier dienstags und donnerstags erstellt, zusammen mit an Freitagen durchgeführten wöchentlichen und monatlichen Backups. Beachten Sie, dass um **Freitag** im Feld **Wöchentlich/monatlich** auswählen zu können, Sie ihn zuerst im Feld **Backup an** auswählen müssen.

Ein solches Archiv würde es Ihnen erlauben, Ihre Finanzdokumente vom ersten und letzten Tag der Arbeit zu vergleichen und eine fünfjährige Geschichte aller Dokumente zu haben.

Keine täglichen Backups

Betrachten Sie ein exotischeres GVS-Schema:

- Backup starten: **12:00 Uhr**
- Sichern: **Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Ein Backup wird daher nur freitags durchgeführt. Dies macht Freitag zur einzigen Wahl für wöchentliche und monatliche Backups, ohne dass ein Tag für tägliche Backups bleibt. Das resultierende „Großvater-Vater“-Archiv wird daher nur aus wöchentlichen differentiellen und monatlichen vollständigen Backups bestehen.

Obwohl es möglich ist, GVS für die Erstellung eines solchen Archivs zu verwenden, ist das eigene Schema in dieser Situation flexibler.

4.2.6.3 Benutzerdefiniertes Backup-Schema

Auf einen Blick

- benutzerdefinierte Planung und Bedingungen für Backups jeden Typs
- Benutzerdefinierte Planungen und Aufbewahrungsregeln

Parameter

Parameter	Bedeutung
Planung für vollständige Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein Voll-Backup durchgeführt werden soll. Ein Beispiel: Das Voll-Backup kann zur Ausführung an jedem Sonntag um 1:00 Uhr angesetzt werden, sobald alle Benutzer abgemeldet wurden.
Planung für inkrementelle Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein inkrementelles Backup durchgeführt werden soll. Anstelle des inkrementellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung kein Voll-Backup enthält.
Planung für differentielle Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein differentielles Backup durchgeführt werden soll. Anstelle des differentiellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung keine Voll-Backups enthält.
Archiv bereinigen	Gibt an, wie alte Backups entfernt werden sollen: entweder durch das regelmäßige Anwenden von Aufbewahrungsregeln (S. 83) oder durch das Bereinigen des Archivs während eines Backups, wenn am Zielspeicherort kein Platz mehr verfügbar ist. Standardmäßig sind keine Aufbewahrungsregeln angegeben und alte Backups daher nicht automatisch gelöscht. **Aufbewahrungsregeln verwenden** Spezifizieren Sie die Aufbewahrungsregeln und wann diese angewendet werden sollen. Diese Einstellung empfiehlt sich für Backup-Ziele wie etwa freigegebene Ordner. **Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist** Das Archiv wird nur während eines Backups bereinigt, sofern nicht ausreichend Speicherplatz für ein neues Backup vorhanden ist. In diesem Fall verhält sich die Software folgendermaßen: ▪ Das älteste Voll-Backup einschließlich aller abhängigen inkrementellen bzw. differentiellen Backups wird gelöscht ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein neues Voll-Backup gerade erstellt wird, dann wird das letzte vollständige Backup mit allen abhängigen inkrementellen bzw. differentiellen Backups gelöscht. ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein inkrementelles bzw. differentielles Backup gerade erstellt wird, erscheint eine Fehlermeldung, dass nicht genügend freier Speicher vorhanden ist. Diese Einstellung empfiehlt sich bei der Sicherung auf einem USB-Laufwerk oder der Acronis Secure Zone. Die Einstellung ist nicht auf FTP- und SFTP-Server anwendbar. Mit dieser Einstellung kann das letzte Backup im Archiv gelöscht werden, falls auf dem Speichermedium nicht ausreichend Platz für mehr als ein Backup vorhanden ist. Bedenken Sie jedoch, dass Ihnen damit möglicherweise kein Backup bleibt, falls das Programm aus irgendeinem Grund das neue Backup nicht erstellen kann.

Aufbewahrungsregeln anwenden (nur wenn Aufbewahrungsregeln erstellt wurden)	Spezifiziert, wann die Aufbewahrungsregeln (S. 83) angewendet werden. Die Bereinigungsprozedur kann z.B. so aufgesetzt werden, dass sie nach jedem Backup und zudem nach Zeitplanung abläuft. Diese Option ist nur dann verfügbar, wenn Sie wenigstens eine Regel in den **Aufbewahrungsregeln** definiert haben.
Planung für Bereinigung (nur wenn **Nach Planung** ausgewählt ist)	Spezifiziert einen Zeitplan zur Bereinigung des Archivs. Die Bereinigung kann z.B. so definiert werden, dass sie planmäßig am letzten Tag eines jeden Monats startet. Diese Option ist nur verfügbar, wenn Sie **Nach Planung** unter **Aufbewahrungsregeln anwenden** gewählt haben.
2. Speicherort, **3. Speicherort**, usw.	Spezifiziert, wohin die Backups vom aktuellen Speicherort aus kopiert oder verschoben (S. 79) werden sollen. Diese Option ist nur verfügbar, wenn Sie entweder das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** unter **Art des Backups** aktiviert haben – oder das Kontrollkästchen **Die ältesten Backups an einen anderen Speicherort verschieben** im Fenster **Aufbewahrungsregeln**.

Beispiele

Wöchentliches Voll-Backup

Das folgende Schema bringt ein Voll-Backup hervor, das jede Freitagnacht erstellt wird.

Voll-Backup: **Planung: Wöchentlich** jeden **Freitag** um **22:00 Uhr**

Hier werden alle Parameter außer **Planung** bei **Voll-Backup** leer gelassen. Alle Backups in diesem Archiv werden unbegrenzt behalten (es wird keine Bereinigung des Archivs vorgenommen).

Voll- und inkrementelles Backup plus Bereinigung

Mit dem nachfolgenden Schema wird das Archiv aus wöchentlichen Voll-Backups und täglichen inkrementellen Backups bestehen. Eine zusätzliche Bedingung ist, dass ein Voll-Backup nur startet, wenn sich alle Benutzer abgemeldet haben.

Voll-Backup: Planung: Wöchentlich jeden **Freitag** um **22:00 Uhr**

Voll-Backup: Bedingungen: Benutzer ist abgemeldet

Inkrementell: Planung: Wöchentlich, an jedem Werktag um **21:00 Uhr**

Weiterhin sollen alle Backups, die älter als ein Jahr sind, aus dem Archiv gelöscht und die Bereinigung nach Erstellung eines neuen Backups durchgeführt werden.

Aufbewahrung: Lösche Backups älter als **12 Monate**

Aufbewahrungsregeln anwenden: Nach Backup

Vorgegeben ist, dass einjährige Backups solange nicht gelöscht werden, bis alle davon abhängenden inkrementellen Backups ebenfalls Objekt einer Löschaktion werden. Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 83).

Monatliche Voll-, wöchentliche differentielle und tägliche inkrementelle Backups plus Bereinigung

Dieses Beispiel demonstriert die Verwendung aller im benutzerdefinierten Schema verfügbaren Optionen.

Angenommen, Sie benötigen ein Schema, das monatliche Voll-Backups, wöchentliche differentielle und tägliche inkrementelle Backups produziert. Die Backup-Planung sieht dann wie folgt aus.

Voll-Backup: Planung: Monatlich jeden **letzten Sonntag** des Monats um **21:00 Uhr**

Inkrementell: Planung: Wöchentlich jeden **Werktag** um **19:00 Uhr**

Differentiell: Planung: Wöchentlich jeden **Samstag** um **20:00 Uhr**

Weiterhin wollen Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit ein Backup-Task startet. Diese werden im Feld **Bedingungen** für jeden Backup-Typ eingestellt.

Voll-Backup: **Bedingungen**: **Speicherort verfügbar**

Inkrementell: **Bedingungen**: **Benutzer ist abgemeldet**

Differentiell: **Bedingungen**: **Benutzer ist untätig**

Als Folge startet ein Voll-Backup – ursprünglich für 21:00 geplant – möglicherweise später: sobald der Backup-Speicherort verfügbar wird. Vergleichbar warten die Backup-Tasks für inkrementelle bzw. differentielle Backups solange, bis alle Benutzer abgemeldet bzw. untätig sind.

Abschließend erstellen Sie Aufbewahrungsregeln für das Archiv: Behalten Sie nur Backups, die nicht älter als sechs Monate sind, und lassen Sie die Bereinigung nach jedem Backup-Task sowie an jedem letzten Tag eines Monats ausführen.

Aufbewahrungsregeln: Lösche Backups älter als **6 Monate**

Aufbewahrungsregeln anwenden: **Nachdem Backup**, **nach Planung**

Planung für die Bereinigung: **Monatlich** am **letzten Tag** von **allen Monaten** um **22:00 Uhr**

Standardmäßig wird ein Backup solange nicht gelöscht, wie es abhängige Backups hat, die behalten werden müssen. Wird z.B. ein Voll-Backup einer Löschaktion unterworfen, während es noch inkrementelle oder differentielle, von ihm abhängende Backups gibt, so wird die Löschung solange verschoben, bis alle abhängenden Backups ebenfalls gelöscht werden können.

Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 83).

4.2.6.4 Schema 'Türme von Hanoi'

Auf einen Blick

- bis zu 16 Level mit vollständigen, differentiellen und inkrementellen Backups
- Backups des nächsten Levels sind doppelt so selten wie die des vorherigen Levels
- Es wird jeweils ein Backup eines Levels gespeichert.
- eine höhere Dichte hin zu jüngeren Backups

Parameter

Sie können beim Schema Türme von Hanoi die folgenden Parameter einstellen.

Planung	Einen täglichen (S. 68), wöchentlichen (S. 70) oder monatlichen (S. 72) Zeitplan einstellen. Bei der Konfiguration von Planungseinstellungen haben Sie auch die Möglichkeit, einfache Planungen zu erstellen (beispielsweise eine einfache tägliche Planung: ein Backup-Task wird täglich um 10 Uhr ausgeführt) – genauso wie auch komplexere Zeitpläne (Beispiel für einen komplexen täglichen Plan: ein Task wird jeden dritten Tag ausgeführt, beginnend vom 15. Januar. An den betreffenden Tagen wird der Task alle 2 Stunden von 10:00 bis 22:00 Uhr wiederholt). Auf diese Weise spezifizieren komplexe Zeitpläne die Sitzungen, an denen das Schema ausgeführt werden soll. In der nachfolgenden Betrachtung können „Tage" durch „geplante Sitzungen" ersetzt werden.
Zahl der Level	Bestimmen Sie zwischen 2 bis 16 Backup-Level. Zu Details siehe die nachfolgend dargestellten Beispiele.
Roll-Back-Zeitspanne	Garantierte Zahl von Sitzungen, die Sie jederzeit im Archiv zurückgehen können. Automatisch kalkuliert, abhängig von den Zeitplan-Parametern und der gewählten Level-Zahl. Zu Details siehe das nachfolgend dargestellte Beispiel.
Backup-Typ	Spezifiziert, welche Backup-Typen die Backup-Level haben werden ▪ **Immer vollständig** – alle Level der Backups werden vom Typ 'Vollständig' sein. Das ist die Standardauswahl für Fälle, in denen ein Bandgerät als Backup-Speicherort ausgewählt wird. ▪ **Vollständig/Differentiell/Inkrementell** – die Backups verschiedener Level werden verschiedene Typen haben: – Backups des letzten Levels sind vollständig – Backups zwischenzeitlicher Level sind differentiell – Backups des ersten Levels sind inkrementell

Beispiel

Die **Zeitplan**-Parameter sind wie folgt eingestellt

- Wiederholen: Jeden Tag
- Frequenz: Einmalig um 18:00 Uhr

Zahl der Level: 4

Backup-Typ: Vollständig/Differentiell/Inkrementell

So sieht der Zeitplan der ersten 14 Tage (oder 14 Sitzungen) für dieses Schema aus. Schattierte Zahlen kennzeichnen die Backup-Level.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Backups unterschiedlicher Level haben unterschiedliche Typen:

- *Letzte-Ebene*-Backups (hier Ebene 4) sind Voll-Backups;
- Die Backups *zwischenzeitlicher Ebenen* (2, 3) sind differentiell;
- *Erste-Ebene* -Backups (1) sind inkrementell.

Ein Bereinigungsmechanismus stellt sicher, dass nur die jeweils neusten Backups jeder Ebene behalten werden. So sieht das Archiv am 8. Tag aus, ein Tag vor Erstellung eines neuen Voll-Backups.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Das Schema erlaubt eine effiziente Datenspeicherung: mehr Backups sammeln sich zur gegenwärtigen Zeit hin an. Mit vier Backups können Sie die Daten von heute, gestern, vor einer halben oder einer ganzen Woche wiederherstellen.

Roll-Back-Zeitspanne

Die Zahl der Tage, die Sie im Archiv zurückgehen können, variiert in Abhängigkeit von den Tagen: Die garantiert verfügbare, minimale Zahl an Tagen wird Roll-Back Periode genannt.

Die nachfolgende Tabelle zeigt Voll-Backups und Roll-Back Perioden für Schemata mit unterschiedlichen Leveln.

Zahl der Level	Voll-Backup alle	Zurück an unterschiedlichen Tagen	Roll-Back-Zeitspanne
2	2 Tage	1 bis 2 Tage	1 Tag
3	4 Tage	2 bis 5 Tage	2 Tage
4	8 Tage	4 bis 11 Tage	4 Tage
5	16 Tage	8 bis 23 Tage	8 Tage
6	32 Tage	16 bis 47 Tage	16 Tage

Durch Hinzufügen eines Levels werden Voll-Backup und Roll-back-Perioden jeweils verdoppelt.

Warum die Zahl von Wiederherstellungstagen variiert, ergibt sich aus dem vorherigen Beispiel.

Das sind die verfügbaren Backups am 12. Tag (Zahlen in Grau kennzeichnen gelöschte Backups).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Das Backup vom 5. Tag liegt immer noch vor, weil bisher kein neues differentielles Backup für Level 3 erstellt wurde. Da es auf dem Voll-Backup von Tag 1 basiert, ist dieses Backup ebenfalls verfügbar. Dies ermöglicht es, bis zu 11 Tage zurückzugehen, was dem Best-Case-Szenario entspricht.

Am folgenden Tag wird jedoch ein neues differentielles Backup der dritten Ebene erstellt und das alte Voll-Backup gelöscht.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

Dies ermöglicht nur ein Wiederherstellungs-Intervall von 4 Tagen, was dem Worst-Case-Szenario entspricht.

Am Tag 14 beträgt das Intervall 5 Tage. Es steigt an den nachfolgenden Tagen, bevor es wieder abnimmt – und so weiter.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Roll-Back-Periode verdeutlicht, wie viele Tage auch im schlimmsten Fall garantiert verfügbar sind. Bei einem Vier-Level-Schema beträgt sie vier Tage.

4.2.6.5 Manueller Start

Mit dem Schema **Manueller Start** müssen Sie keine Backup-Planung spezifizieren. Sie können den Backup-Plan von der Ansicht **Pläne und Tasks** jederzeit später manuell ausführen.

Spezifizieren Sie die passenden Einstellungen wie folgt.

Backup-Typ

Wählen Sie den Typ des Backups

- **Vollständig** – Standardmäßig für alle Backup-Speicherorte (mit Ausnahme des Acronis Cloud Storages) vorausgewählt.
- **Inkrementell.** Beim ersten Mal wird ein Voll-Backup erstellt. Die nachfolgenden Backups werden inkrementell. Als einziger Backup-Typ für den Acronis Cloud Storage ausgewählt.
- **Differentiell.** Beim ersten Mal wird ein Voll-Backup erstellt. Die nächsten Backups werden differentiell.

4.2.6.6 Initial Seeding

Dieses Backup-Schema ist verfügbar, wenn der Acronis Cloud Storage als Backup-Ziel ausgewählt wurde. Ein Backup ist nur dann erfolgreich, wenn Sie eine Initial Seeding-Lizenz haben.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Initial Seeding ermöglicht Ihnen, das erste Backup (üblicherweise ein Voll-Backup und sehr groß) durch Verwendung einer Festplatte (oder ähnlichen Laufwerks) statt per Internetübertragung zum Cloud Storage hochzuladen. Nachfolgende Backups (üblicherweise inkrementell und daher deutlich kleiner) können dann per Internet übertragen werden, sobald das Voll-Backup im Cloud Storage angekommen ist.

Wenn Sie eine Datenmenge von 100 GB oder mehr sichern, ermöglicht Initial Seeding eine schnellere Auslieferung der Daten und geringere Übertragungskosten.

Konsultieren Sie zu weiteren Details den Abschnitt „Initial Seeding FAQ (S. 275)“.

4.2.7 Archiv-Validierung

Setzen Sie einen Validierungstask auf, um zu überprüfen, ob gesicherte Daten wiederherstellbar sind. Der Validierungstask scheitert und der Backup-Plan erhält den Status **Error**, wenn das Backup die Überprüfung nicht erfolgreich bestehen konnte.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Image-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist.

Spezifizieren Sie die folgenden Parameter, um eine Validierung anzulegen

1. **Validierungszeitpunkt** – bestimmen Sie, wann die Validierung durchgeführt wird. Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu **planen**, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Wenn die Validierung dagegen ein wichtiger Teil Ihrer Strategie zur Datensicherung ist und Sie es bevorzugen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, dann sollten Sie die Validierung direkt nach Backup-Erstellung durchführen.
2. **Was validieren** – bestimmen Sie, ob das komplette Archiv oder das letzte Backup im Archiv überprüft wird.

   Die Validierung eines Archivs überprüft alle Backups des Archivs und kann viel Zeit sowie System-Ressourcen benötigen.

Die Validierung des letzten Backups kann auch Zeit benötigen, selbst wenn dieses Backup inkrementell oder differentielle ist und nur eine geringe Größe hat. Hintergrund ist, dass die Aktion nicht einfach nur die konkret im Backup enthaltenen Daten validiert, sondern alle durch Wahl des Backups wiederherstellbaren Daten. Dies erfordert einen Zugriff auf zuvor erstellte Backups.

3. **Validierungsplanung** (erscheint nur, falls Sie in Schritt 1 **Nach Zeitplan** ausgewählt haben) – definiert den Zeitplan für die Validierung. Zu weiteren Informationen siehe den Abschnitt Planung (S. 66).

4.2.8 Anmeldedaten des Backup-Plans

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, unter dem der Plan ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Acronis Service verwenden** oder **Unter dem aktuellen Benutzer ausführen**

     Der Plan wird unter einem der folgenden Benutzerkonten ausgeführt:
     - Das Konto des Agenten-Dienstes (Agent Service), sofern Sie administrative Berechtigungen auf der Maschine haben.
     - Ihr Konto, sofern Sie als normaler Benutzer angemeldet sind (etwa als Mitglied der Gruppe 'Benutzer').
   - **Folgende Anmeldedaten verwenden**

     Die Tasks werden immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 25), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

4.2.9 Bezeichnung (Maschinen-Eigenschaften in einem Backup bewahren)

Jedes Mal, wenn eine Maschine gesichert wird, werden dem Backup auch Informationen über den Maschinennamen, das Betriebssystem, das Windows Service Pack sowie den 'Security Identifier' (SID) hinzugefügt – ergänzt um eine benutzerdefinierte Textbezeichnungen. Die Bezeichnung kann Angaben zur Abteilung, zum Namen des Maschinen-Benutzers oder ähnliche Informationen enthalten, die als Kennzeichnung (Tag) oder Suchschlüssel dienen können.

Wenn Sie die Maschine mit dem Agenten für VMware zu einem VMware ESX(i)-Server wiederherstellen (S. 112) oder das Backup zu einer virtuellen ESX(i)-Maschine konvertieren (S. 153), dann werden diese Eigenschaften in die Konfiguration der virtuellen Maschine übertragen. Sie können diese dann in den Einstellungen der virtuellen Maschine einsehen: **Einstellungen bearbeiten**

–> **Optionen** –> **Erweitert** –> **Allgemein** –> **Konfigurationsparameter**. Sie können die virtuellen Maschinen mit Hilfe dieser einstellbaren Parameter sortieren oder gruppieren. Das kann bei verschiedenen Szenarien nützlich sein.

Beispiel:

Angenommen, Sie möchten Ihr Büro oder Datacenter in eine virtuelle Umgebung migrieren. Sie können durch die Verwendung von Dritthersteller-Software, die per VMware-API auf die Konfigurationsparameter zugreifen kann, Sicherheitsrichtlinien auf jede Maschine anwenden – sogar bevor diese eingeschaltet wird.

So fügen Sie Backups eine Textbezeichnung hinzu:

1. Klicken Sie auf der Seite **Backup-Plan erstellen** (S. 38) auf **Anmeldedaten des Plans, Kommentare, Bezeichnung anzeigen**.
2. Geben Sie im Feld **Bezeichnung** die gewünschte Benennung ein – oder wählen Sie eine aus dem aufklappbaren Menü aus.

Spezifikation der Parameter

Parameter	Wert	Beschreibung
acronisTag.label	<string>	Eine benutzerdefinierte Bezeichnung. Die Bezeichnung kann von einem Benutzer bei Erstellung eines Backup-Plans festgelegt werden.
acronisTag.hostname	<string>	Host-Name (FQDN)
acronisTag.os.type	<string>	Betriebssystem
acronisTag.os.servicepack	0, 1, 2...	Die Version des im System installierten Service Packs. Nur für Windows-Betriebssysteme.
acronisTag.os.sid	<string>	Die SID der Maschine. Beispielsweise: S-1-5-21-874133492-782267321-3928949834. Nur für Windows-Betriebssysteme.

Werte des Parameters 'acronisTag.os.type'

Windows NT 4	winNTGuest
Windows 2000 Professional	win2000ProGuest
Windows 2000 Server	win2000ServGuest
Windows 2000 Advanced Server	win2000ServGuest
Windows XP – alle Editionen	winXPProGuest
Windows XP – All Editionen (64 Bit)	winXPPro64Guest
Windows Server 2003 – alle Editionen	winNetStandardGuest
Windows Server 2003 – All Editionen (64 Bit)	winNetStandard64Guest
Windows 2008	winLonghornGuest
Windows 2008 (64 Bit)	winLonghorn64Guest
Windows Vista	winVistaGuest
Windows Vista (64 Bit)	winVista64Guest
Windows 7	windows7Guest

Windows 7 (64 Bit)	windows7_64Guest
Windows Server 2008 R2 (64 Bit)	windows7Server64Guest
Linux	otherLinuxGuest
Linux (64 Bit)	otherLinux64Guest
Anderes Betriebssystem	otherGuest
Anderes Betriebssystem (64 Bit)	otherGuest64

Beispiel

acronisTag.label = "DEPT:BUCH; COMP:SUPERSERVER; OWNER:EJONSON"

acronisTag.hostname = "superserver.corp.local"

acronisTag.os.type = "windows7Server64Guest"

acronisTag.os.servicepack = "1"

acronisTag.os.sid = "S-1-5-21-874133492-782267321-3928949834"

4.2.10 Die Reihenfolge von Aktionen in einem Backup-Plan

Falls ein Backup-Plan mehrere Aktionen enthält, führt Acronis Backup diese in folgender Reihenfolge aus:

1. Bereinigung (falls **Vor dem Backup** konfiguriert) und Validierung (falls die Bereinigung ausgeführt wurde und die Validierung zur Ausführung **Nach Anwendung der Aufbewahrungsregeln** konfiguriert ist).

   Falls ein Backup während der Bereinigung zu einem anderen Speicherort verschoben wurde, werden alle Aktionen, die für die nachfolgenden Speicherort konfiguriert wurden, zuerst durchgeführt, bevor mit den nachfolgenden Schritten für den primären Speicherort fortgefahren wird.
2. Befehlsausführung vor dem Backup.
3. Backup:
   a. Befehlsausführung vor Datenerfassung
   b. Snapshot-Erstellung
   c. Befehlsausführung nach Datenerfassung
   d. Backup-Prozess
4. Start der Backup-Katalogisierung

   Die Backup-Katalogisierung kann ein zeitaufwendiges Verfahren sein. Sie wird parallel mit den nachfolgenden Schritten ausgeführt.
5. Befehlsausführung nach dem Backup.
6. Desaster-Recovery-Plan (DRP)-Erstellung.
7. Konvertierung zu einer virtuellen Maschine.
8. Backup-Replikation.
9. Bereinigung.

   Falls die Replikation stattgefunden hat oder ein Backup während der Bereinigung zu einem anderen Speicherort verschoben wurde, werden alle Aktionen, die für die nachfolgenden Speicherort konfiguriert wurden, zuerst durchgeführt, bevor mit den nachfolgenden Schritten für den primären Speicherort fortgefahren wird.
10. Validierung.
11. Bandauswurf.

12. Versenden von E-Mail-Benachrichtigung.

4.2.11 Warum fragt das Programm nach einem Kennwort?

Ein geplanter oder aufgeschobener Task muss unabhängig davon, ob ein Benutzer angemeldet ist, ausgeführt werden. In Fällen, in denen Sie die Anmeldedaten, unter denen ein Task ausgeführt wird, nicht explizit angegeben haben, schlägt das Programm die Verwendung Ihres Benutzerkontos vor. Geben Sie Ihr Kennwort ein, spezifizieren Sie ein anderes Konto oder ändern Sie die geplante Ausführung auf manuell.

4.3 Vereinfachte Benennung von Backup-Dateien

Gehen Sie folgendermaßen vor, um die vereinfachte Benennung von Backup-Dateien verwenden zu können:

- Klicken Sie in der Willkommensseite auf **Backup-Plan erstellen** (S. 38), erweitern Sie **Benennung der Backup-Datei, Archivkommentare anzeigen** und aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.

  Wenn Sie ein Backup von einem lokal angeschlossenen RDX- oder USB-Flash-Laufwerk erstellen, erscheint das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht. Stattdessen bestimmt der Wechsellaufwerksmodus (S. 170), ob das Standard- oder das vereinfachte Bennenungsschema verwendet wird. Unter Linux erscheint das Kontrollkästchen, nachdem Sie das Gerät manuell gemountet haben.
- Klicken Sie in der Willkommensseite auf **Backup jetzt** (S. 38). Die 'vereinfachte Benennung' wird immer dann verwendet, wenn das Backup-Ziel dies unterstützt (zu den Beschränkungen siehe weiter unten).

Wenn Sie die vereinfachte Dateibenennung verwenden, gilt:

- Der Dateiname des ersten (vollständigen) Backups im Archiv wird aus dem Archivnamen zusammengesetzt, beispielsweise: **MeineDateien.tib.** Die Dateinamen der nachfolgenden (inkrementellen oder differentiellen) Backups erhalten eine zusätzliche Kennziffer. Beispielsweise: **MeineDateien2.tib**, **MeineDateien3.tib** und so weiter.

  Diese einfache Namensschema ermöglicht Ihnen, von einer Maschine ein 'transportierbares' Image auf ein entfernbares Medium zu erstellen – oder die Backups durch Verwendung eines Skripts an einen anderen Speicherort zu verschieben.
- Die Software löscht vor Erstellung eines neuen Voll-Backups das komplette Archiv und startet danach ein neues.

  Dieses Verhalten ist nützlich, wenn Sie mehrere USB-Festplatten abwechselnd verwenden und jedes Laufwerk ein einzelnes Voll-Backup (S. 64) oder alle während einer Woche erstellten Backups (S. 65) behalten soll. Sie könnten am Ende aber ganz ohne Backups dastehen, falls ein Voll-Backup zu Ihrem einzigen Laufwerk fehlschlägt.

  Dieses Verhalten lässt sich aber unterdrücken, wenn Sie dem Archivnamen die [Datum]-Variable (S. 62) hinzufügen.

Wenn Sie die Standard-Dateibenennung verwenden, gilt:

- Jedes Backup erhält einen eindeutigen Dateinamen mit exaktem Datumsstempel und Backup-Typ. Beispielsweise: **MeineDateien_2010_03_26_17_01_38_960D.tib**. Diese Standard-Dateibenennung ermöglicht eine weitreichendere Nutzung von Backup-Zielorten und Backup-Schemata.

Einschränkungen

Bei Verwendung der vereinfachten Dateibenennung ist folgende Funktionalität nicht verfügbar:

- Konfiguration vollständiger, inkrementeller und differentieller Backups innerhalb eines einzigen Backup-Plans. Sie müssen separate Backup-Pläne für jeden Backup-Typ erstellen.
- Backups auf ein Band, in die Acronis Secure Zone oder den Acronis Cloud Storage.
- Replikation von Backups einrichten
- Aufbewahrungsregeln konfigurieren
- Regelmäßige Konvertierung von Backups zu einer virtuellen Maschine einrichten
- Konvertierung eines inkrementellen oder differentiellen Backups zu einem Voll-Backup

Beschränkungen bei Archivnamen

- Ein Archivname darf nicht mit einer Zahl enden.
- Folgende Zeichen sind bei FAT16-, FAT32- und NTFS-Dateisystemen für Dateinamen nicht erlaubt: Backslash (\), Schrägstrich (/), Doppelpunkt (:), Sternchen (Asterisk) (*), Fragezeichen (?), Anführungszeichen ("), Kleiner-als-Zeichen (<), Größer-als-Zeichen (>) und Hochstrich (|).

4.3.1 Die Variable '[DATE]'

Wenn Sie die Variable **[DATE]** zur Verwendung im Archivnamen spezifizieren, enthält der Dateiname eines jeden Backups sein entsprechendes Erstellungsdatum.

Bei Verwendung dieser Variable wird das erste Backup eines neuen Tages ein Voll-Backup. Die Software löscht vor Erstellung des nächsten Voll-Backups alle schon früher an diesem Tag erstellten Backups. Backups, die vor diesem Tag erstellt wurden, bleiben erhalten. Das bedeutet, dass Sie multiple Voll-Backups (mit oder ohne inkrementelle Erweiterungen) speichern können, jedoch nicht mehr als ein Voll-Backup pro Tag. Sie können die Backups nach Datum sortieren lassen. Sie können außerdem ein Skript verwenden, um ältere Backups zu kopieren, verschieben oder löschen.

Der Wert dieser Variablen ist das aktuelle Datum, eingefasst von Klammern ([]). Das Datumsformat hängt von den regionalen Einstellungen Ihrer Maschine ab. Falls das Datumsformat beispielsweise *Jahr-Monat-Tag* ist, dann ergibt der 31. Januar 2012 den Wert **[2012-01-31]**. Zeichen, die in Dateinamen nicht unterstützt werden (wie etwa Schrägzeichen (/)) werden durch Unterstriche (_) ersetzt.

Sie können die Variable an jeder Stelle im Archivnamen positionieren. Sie können zudem Groß- und Kleinbuchstaben in dieser Variable verwenden.

Beispiele

Beispiel 1: Angenommen Sie führen für zwei Tage, startend am 31.01.2012, zweimal täglich inkrementelle Backups aus (um Mitternacht und zur Mittagszeit). Der Archivname ist **MeinArchiv-[DATE]**, das Datumsformat ist *Jahr-Monat-Tag.* So sieht die Liste der Backup-Dateien nach dem zweiten Tag aus:

MeinArchiv-[2012-01-31].tib (vollständig, erstellt am 31. Januar um Mitternacht)
MeinArchiv-[2012-01-31]2.tib (inkrementell, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-[2012-02-01].tib (vollständig, erstellt am 1. Februar um Mitternacht)
MeinArchiv-[2012-02-01]2.tib (inkrementell, erstellt am 1. Februar, zur Mittagszeit)

Beispiel 2: Angenommen, Sie erstellen Voll-Backups mit gleicher Planung, gleichem Archivnamen und Datumsformat wie im vorherigen Beispiel. In diesem Fall sieht die Liste der Backup-Dateien nach dem zweiten Tag wie folgt aus:

MeinArchiv-[2012-01-31].tib (vollständig, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-[2012-02-01].tib (vollständig, erstellt am 1. Februar, zur Mittagszeit)

Hintergrund des Ergebnisses ist, dass die um Mitternacht erstellten Voll-Backups durch am selben Tag neu erstellte Voll-Backups ersetzt werden.

4.3.2 Backup-Aufteilung und vereinfachte Dateibenennung

Wenn ein Backup entsprechend der Einstellungen unter Backup-Aufteilung (S. 93) aufgesplittet wird, dann wird die gleiche Indizierung auch für die Namensteile des Backups verwendet. Der Dateiname für das nächste Backup erhält den nächsten verfügbaren Index.

Angenommen, das erste Backup des Archives **MeineDateien** wurde in zwei Teile aufgeteilt. Die Dateinamen dieses Backups sind folglich **MeineDateien1.tib** und **MeineDateien2.tib**. Das zweite Backup (als nicht aufgeteilt angenommen) wird **MeineDateien3.tib** genannt.

4.3.3 Verwendungsbeispiele

Dieser Abschnitt zeigt Ihnen Beispiele für die Verwendung der vereinfachten Dateibenennung.

4.3.3.1 Beispiel 1: Tägliches Backup ersetzt das alte

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie wollen das Backup auf einer lokal angeschlossenen USB-Festplatte in der Datei **MeineMaschine.tib** speichern.
- Sie wollen, dass jedes neue Backup das jeweilige alte ersetzt.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans die USB-Festplatte als Archiv-Speicherort und **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis. Das Archiv besteht aus einer einzigen Datei: MeineMaschine.tib. Diese Datei wird vor Erstellung eines neuen Backups wieder gelöscht.

Falls Sie ein lokal angeschlossenes RDX-Laufwerk oder USB-Flash-Laufwerk zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 170) auf **Wechselmedien** eingestellt ist.

4.3.3.2 Beispiel 2: Tägliche Voll-Backups mit Datumsstempel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie möchten ältere Backups per Skript zu einem Remote-Speicherort verschieben.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis:

- Die Backups vom 1. Januar 2012, 2. Januar 2012 (usw.) werden entsprechend als 'MeineMaschine-[2012-01-01].tib', 'MeineMaschine-[2012-01-02].tib' (usw.) gespeichert.
- Ihr Skript kann ältere Backups auf Basis des Datumsstempels verschieben.

Siehe auch „Die Variable [Date]“ (S. 62).

4.3.3.3 Beispiel 3: Stündliche Backups innerhalb eines Tages

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag stündliche Backups erstellen.
- Das erste Backup eines jeden Tages soll 'vollständig' sein und um Mitternacht ausgeführt werden – die nachfolgenden Backups des Tages sollen differentiell sein und um 01:00 Uhr, 02:00 Uhr (usw.) ausgeführt werden.
- Ältere Backups sollen im Archiv aufbewahrt werden.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **ServerDateien[Date]** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Differentiell** als Backup-Typ fest – und planen Sie dann für die Backups eine stündliche Ausführung (ab Mitternacht).

Ergebnis:

- Die 24 Backups vom 01.01.2012 werden als 'ServerDateien[2012-01-01].tib', 'ServerDateien[2012-01-01]2.tib' (usw.) bis zu 'ServerDateien[2012-01-01]24.tib' gespeichert.
- Die Backups des folgenden Tags starten mit einem Voll-Backup namens 'ServerDateien[2012-01-02].tib'.

Siehe auch „Die Variable [Date]“ (S. 62).

4.3.3.4 Beispiel 4. Tägliche Voll-Backups mit täglichem Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie wollen das Backup auf einer lokal angeschlossenen USB-Festplatte in der Datei **MeineMaschine.tib** speichern.
- Sie haben zwei dieser Laufwerke. Jedes verwendet beim Anschluss an die Maschine den Laufwerksbuchstaben **D**.
- Sie möchten die Laufwerke vor jedem Backup wechseln, so dass eines der Laufwerke die Backups von heute enthält, das andere die von gestern.
- Jedes neue Backup soll das Backup auf dem aktuell angeschlossenen Laufwerk ersetzen.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Bei Erstellung des Backup-Plans:

- Spezifizieren Sie **MeineMachine** als Archivnamen.
- Spezifizieren Sie **D:** als Archiv-Speicherort.
- Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.

- Wählen Sie **Vollständig** als Backup-Typ.

Ergebnis: Jedes Laufwerk wird nur je ein Voll-Backup enthalten. Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Falls Sie lokal angeschlossene RDX-Laufwerke oder USB-Flash-Laufwerke zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 170) auf **Wechselmedien** eingestellt ist.

4.3.3.5 Beispiel 5. Tägliche Voll-Backups mit wöchentlichen Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit täglichen Backups sichern: ein Voll-Backup an jedem Montag und inkrementelle Backups von Dienstag bis Sonntag.
- Sie wollen die Backups auf einer lokal angeschlossenen USB-Festplatte im Archiv **MeineMaschine.tib** speichern.
- Sie haben zwei dieser Laufwerke. Jedes verwendet beim Anschluss an die Maschine im Betriebssystem den Laufwerksbuchstaben **D**.
- Die Laufwerke sollen an jedem Montag gewechselt werden, so dass ein Laufwerk die Backups der aktuellen Woche (Montag bis Sonntag) enhält – und das andere Laufwerk die Backups der letzten Woche.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Bei Erstellung des ersten Backup-Plans:
   - Spezifizieren Sie **MeineMachine** als Archivnamen.
   - Spezifizieren Sie **D:** als Archiv-Speicherort, wobei **D** der Laufwerksbuchstabe ist, den jedes der Laufwerke nach Anschluss an die Maschine im Betriebssystem hat.
   - Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.
   - Wählen Sie **Vollständig** als Backup-Typ.
   - Planen Sie die Backups so, dass Sie jede Woche am Montag laufen.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Inkrementell** als Backup-Typ wählen und für die Backups eine wöchentliche Ausführung von Dienstag bis Sonntag planen.

Ergebnis:

- Bevor das 'Montags-Backup' erstellt wird (durch den ersten Backup-Plan), werden alle auf dem aktuell angeschlossenen Laufwerk liegenden Backups gelöscht.
- Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Falls Sie lokal angeschlossene RDX-Laufwerke oder USB-Flash-Laufwerke zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 170) auf **Wechselmedien** eingestellt ist.

4.3.3.6 Beispiel 6: Backups während der Arbeitszeit

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag Backups erstellen.
- Das erste Backup eines Tages soll vollständig sein und um 01:00 Uhr ausgeführt werden.
- Die Backups während der Arbeitszeit sollen differentiell sein und stündlich von 8:00 Uhr bis 17:00 Uhr ausgeführt werden.
- Dem Namen einer jeden Backup-Datei soll das Erstellungsdatum hinzugefügt werden.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Spezifizieren Sie bei Erstellung des ersten Backup-Plans **ServerDateien[DATE]** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Voll** als Backup-Typ fest – und planen Sie dann für die Backups eine tägliche Ausführung um 01:00 Uhr.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Differentiell** als Backup-Typ wählen und die Backups folgendermaßen planen:

   - **Task starten**: **täglich**
   - **Alle**: **1 Stunde(n)**
   - **Von**: **08:00:00 Uhr**
   - **Bis**: **17:01:00 Uhr**

Ergebnis:

- Das Voll-Backup vom 31.01.2012 wird als 'ServerDateien[2012-01-31].tib' gespeichert.
- Die 10 differentiellen Backups vom 31.01.2012 werden als 'ServerDateien[2012-01-31]2.tib', 'ServerDateien[2012-01-31]3.tib' (usw.) bis zu 'ServerDateien[2012-01-31]11.tib' gespeichert.
- Die Backups des folgenden Tags (1. Februar) starten mit einem Voll-Backup namens 'ServerDateien[2012-02-01].tib'. Die differentiellen Backups starten mit 'ServerDateien[2012-02-01]2.tib'.

Siehe auch „Die Variable [Date]“ (S. 62).

4.4 Planung

Der Acronis-Scheduler hilft dem Administrator, Backup-Pläne an die tägliche Firmenroutine und den Arbeitsstil eines jeden Angestellten anzupassen. Die Tasks der Pläne werden systematisch so gestartet, dass kritische Daten als sicher geschützt bewahrt werden.

Die Möglichkeit zur Planung steht zur Verfügung, wenn Sie bei Erstellung eines Backup-Plans (S. 38) eines der folgenden Backup-Schemata verwenden: Einfach, Benutzerdefiniert oder 'Türme von Hanoi'. Sie können die Planungsmöglichkeit auch für Validierungstask (S. 172) einstellen.

Der Scheduler verwendet die lokale Zeit der Maschine, auf der der Backup-Plan existiert. Bevor Sie eine Planung erstellen, überprüfen Sie, ob die Datums- bzw. Zeit-Einstellungen der Maschine korrekt sind.

Planung

Sie müssen ein oder mehrere Ereignisse spezifizieren, um zu bestimmen, wann ein Task ausgeführt werden soll. Der Task wird gestartet, sobald eines der Ereignisse eintritt. Die Tabelle führt Ereignisse auf, die unter Windows-Betriebssystemen verfügbar sind.

Ereignis
Zeit: Täglich, Wöchentlich, Monatlich
Verstrichene Zeit, seit das letzte erfolgreiche Backup abgeschlossen wurde. (geben Sie die Zeitdauer an)
Benutzeranmeldung (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an)
Benutzerabmeldung* (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an) *'Herunterfahren' ist nicht dieselbe Aktion wie 'Abmelden'. Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt.
Systemstart
System herunterfahren
Ein Ereignis in der Windows-Ereignisanzeige (spezifizieren Sie die Parameter des Ereignisses)

Bedingung

Nur bei Backup-Aktionen können Sie zusätzlich zu den Ereignissen eine oder mehrere Bedingungen angeben. Sobald eines der Ereignisse eintritt, überprüft der Scheduler die Bedingung und führt den Task aus, falls die Bedingung erfüllt ist. Bei mehreren Bedingungen müssen diese alle gleichzeitig zusammentreffen, um die Task-Ausführung zu ermöglichen. Die Tabelle führt die Bedingungen auf, die unter Windows-Betriebssystemen verfügbar sind.

Bedingung: Task nur starten, wenn
Benutzer ist inaktiv (ein Bildschirmschoner ausgeführt wird oder die Maschine gesperrt ist)
Host des Speicherorts verfügbar ist
Laufzeit des Tasks sich innerhalb des spezifizierten Zeitintervalls befindet
Benutzer alle abgemeldet sind
Zeitperiode verstrichen ist, seit das letzte erfolgreiche Backup abgeschlossen wurde

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option Task-Startbedingungen (S. 108) definiert.

Was ist, wenn

- **Was ist, wenn ein Ereignis eintritt (und eine Bedingung, sofern vorhanden, erfüllt ist), während die Ausführung des vorherigen Tasks noch nicht abgeschlossen ist?**

  Das Ereignis wird ignoriert.
- **Was ist, wenn ein Ereignis eintritt, während der Scheduler auf die Bedingung wartet, die für das vorherige Ereignis benötigt wurde?**

  Das Ereignis wird ignoriert.
- **Was ist, wenn die Bedingung für eine sehr lange Zeit nicht erfüllt wird?**

Wird die Verzögerung eines Backups zu riskant, so können Sie die Bedingung erzwingen (den Benutzer anweisen, sich abzumelden) oder den Task manuell ausführen. Sie können, damit diese Situation automatisiert gehandhabt wird, ein Zeitintervall definieren, nachdem der Task unabhängig von der Bedingung ausgeführt wird.

4.4.1 Tägliche Planung

Tägliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine tägliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Tag(e)	Stellen Sie eine bestimmte Anzahl von Tagen ein, an denen Sie den Task ausgeführt haben wollen. Stellen Sie z.B. „Alle 2 Tage“ ein, so wird der Task an jedem zweiten Tag gestartet.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls erneut gestartet wird. Stellen Sie z.B. die Task-Frequenz auf „Jede 1 Stunde“ von 10:00 Uhr bis 22:00 Uhr ein, so erlaubt dies dem Task, zwölfmal zu laufen: von 10:00 vormittags bis 22:00 abends innerhalb eines Tages.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Tagen.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Einfache“ tägliche Planung

Führe den Task jeden Tag um 18:00 Uhr aus.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Einmal: **18:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**. Der Task wird noch am selben Tag gestartet, sofern er vor 18:00 Uhr erstellt wurde. Wurde der Task nach 18:00 Uhr erstellt, dann wird er das erste Mal am nächsten Tag um 18:00 Uhr gestartet.

   Bis: **nicht eingestellt**. Der Task wird für eine unbegrenzte Zahl an Tagen ausgeführt.

„Drei-Stunden-Zeitintervall über drei Monate“-Planung

Den Task alle drei Stunden ausführen. Der Task startet an einem bestimmten Datum (z.B. 15. September 2009) und endet nach drei Monaten.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Alle: **3** Stunden

   Von: **24:00 Uhr** (Mitternacht) bis: **21:00 Uhr** – der Task wird daher achtmal pro Tag mit einem Intervall von 3 Stunden ausgeführt. Nach der letzten täglichen Wiederholung um 21:00 Uhr kommt der nächste Tag und der Task startet erneut von Mitternacht.
3. Wirksam:

   Von: **15.09.2009**. Wenn der 15.09.2009 das aktuelle Datum der Task-Erstellung ist und z.B. 13:15 Uhr die Erstellungszeit des Tasks, dann wird der Task gestartet, sobald das nächste Zeitintervall kommt: um 15:00 Uhr in unserem Beispiel.

   Bis: **15.12.2009**. An diesem Datum wird der Task das letzte Mal ausgeführt, der Task selbst ist jedoch immer noch in der Ansicht **Tasks** verfügbar.

Mehrere tägliche Planungen für einen Task

Es gibt Fälle, in denen es für Sie notwendig sein kann, den Task mehrmals am Tag laufen zu lassen oder sogar mehrmals am Tag mit unterschiedlichen Zeitintervallen. Erwägen Sie in diesen Fällen, einem Task mehrere Zeitplanungen hinzuzufügen.

Angenommen, der Task soll z.B. jeden dritten Tag ausgeführt werden, beginnend vom 20.09.2009, fünfmal am Tag:

- Zuerst um 8:00 Uhr.
- das zweite Mal um 12:00 Uhr (mittags)
- das dritte Mal um 15:00 Uhr
- das vierte Mal um 17:00 Uhr
- das fünfte Mal um 19:00 Uhr

Der offensichtliche Weg ist es, fünf einfache Zeitplanungen hinzuzufügen. Wenn Sie eine Minute überlegen, können Sie sich einen optimaleren Weg ausdenken. Wie Sie sehen, beträgt das Zeitintervall zwischen der ersten und zweiten Task-Wiederholung 4 Stunden und zwischen der dritten, vierten und fünften sind es 2 Stunden. Für diesen Fall besteht die optimale Lösung darin, dem Task zwei Planungen hinzuzufügen.

Erste tägliche Planung

1. Alle: **3** Tage.
2. Alle: **4** Stunden.

   Von: **08:00:00 Uhr** bis: **12:00 Uhr**.
3. Wirksam:

   Von: **09/20/2009**.

   Bis: **nicht eingestellt**.

Zweite tägliche Planung

1. Alle: **3** Tage.
2. Alle: **2** Stunden.

   Von: **15:00 Uhr** bis: **19:00:00 Uhr**.
3. Wirksam:

   Von: **09/20/2009**.

   Bis: **nicht eingestellt**.

4.4.2 Wöchentliche Planung

Eine wöchentliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine wöchentliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Woche (Wochen) am: <...>	Spezifizieren Sie eine gewisse Zahl von Wochen und die Wochentage, an denen Sie den Task ausführen wollen. Mit einer Einstellung z.B. alle **2** Wochen am **Montag** wird der Task am Montag jeder zweiten Woche ausgeführt.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Wochen.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

'Ein Tag in der Woche'-Planung

Den Task jeden Freitag um 22:00 Uhr ausführen, beginnend mit einem bestimmten Datum (z.B. 14.05.2009) und nach sechs Monaten endend.

Die Parameter der Planung werden wie folgt eingestellt:

1. Jeden: **1** Woche(n) am: **Fr**.
2. Einmal: **22:00:00 Uhr**.
3. Wirksam:

   Von: **13.05.2009**. Der Task wird am nächsten Freitag um 22:00 Uhr gestartet.

   Bis: **13.11.2009**. An diesem Datum wird der Task das letzte Mal ausgeführt, der Task selbst ist jedoch nach diesem Datum immer noch in der Task-Ansicht verfügbar. (Wenn dieser Tag kein Freitag wäre, dann würde der Task zuletzt an dem Freitag ausgeführt werden, der vor diesem Datum liegt.)

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die 'Ein Tag in der Woche'-Planung wird den Voll-Backups hinzugefügt.

'Werktags'-Planung

Den Task jede Woche an Werktagen ausführen: von Montag bis Freitag. Während eines Werktags startet der Task nur einmal um 21:00 Uhr.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Woche(n) am: **<Werktags>** – die Wahl des Kontrollkästchens <Werktags> aktiviert automatisch die korrespondierenden Kontrollkästchen (**Mo**, **Di**, **Mi**, **Do** und **Fr**) und lässt die verbliebenen unverändert.
2. Einmal: **21:00 Uhr**.
3. Wirksam:

   Von: **leer**. Wenn Sie den Task z.B. am Montag um 11:30 Uhr erstellt haben, dann wird er am selben Tag um 21:00 Uhr gestartet. Wurde der Task z.B. am Freitag nach 21:00 Uhr erstellt, dann wird er das erste Mal am nächsten Wochentag (in unserem Beispiel Montag) um 21:00 Uhr gestartet.

   Enddatum: **leer**. Der Task wird für eine unbegrenzte Anzahl an Wochen erneut gestartet.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Wochentags“-Planung wird den inkrementellen Backups hinzugefügt, während das Voll-Backup mit einer Ausführung an einem Tag in der Woche geplant wird. Zu weiteren Details siehe die Beispiele über vollständige und inkrementelle Backups sowie Bereinigungen im Abschnitt Benutzerdefiniertes Backup-Schema (S. 51).

Mehrere wöchentliche Planungen für einen Task

In Fällen, in denen der Task an verschiedenen Tagen der Woche mit verschiedenen Zeitintervallen ausgeführt werden muss, sollten Sie erwägen, jedem gewünschten Tag oder mehreren Tagen der Woche eine geeignete Planung zuzuweisen.

Angenommen, Sie müssen den Task mit der folgenden Planung ausführen:

- Montag zweimal, um 12:00 Uhr (mittags) und 21:00 Uhr
- Dienstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Mittwoch: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Donnerstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Freitag: zweimal, um 12:00 Uhr und 21:00 Uhr (d.h. wie am Montag)
- Samstag: einmal um 21:00 Uhr
- Sonntag: einmal um 21:00 Uhr

Durch Kombinieren der identischen Zeiten können die folgenden drei Planungen dem Task hinzugefügt werden:

Erste Planung

1. Alle: **1** Woche(n) am: **Mo**, **Fr**.
2. Alle: **9** Stunden

   Von: **12:00 Uhr** bis: **21:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**.

   Bis: **nicht eingestellt**.

Zweite Planung

1. Alle **1** Woche(n) am: **Di**, **Mi**, **Do**.
2. Alle **3** Stunden

   Von **09:00 Uhr** bis **21:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**.

Bis: **nicht eingestellt**.

Dritte Planung

1. Alle: **1** Woche(n) am: **Sa, So**.
2. Einmal: **21:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**.

   Bis: **nicht eingestellt**.

4.4.3 Monatliche Planung

Eine monatliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine monatliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Monate: <...>	Wählen Sie den/die Monat(e), in der/denen Sie den Task ausführen wollen.
Tage: <...>	Bestimmen Sie die spezifischen Tage des Monats, um an diesen den Task auszuführen. Sie können außerdem den letzten Tag eines Monats auswählen, unabhängig von seinem tatsächlichem Datum.
Am(Um): <...> <...>	Bestimmen Sie die spezifischen Tage der Wochen, um an diesen den Task auszuführen.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Monaten.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Letzter Tag eines jeden Monats"-Planung

Den Task einmal um 22:00 Uhr am letzten Tag eines jeden Monats ausführen.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **<Alle Monate>**.
2. Tage: **Letzter**. Der Task wird am letzten Tag eines jeden Monats ausgeführt, ungeachtet seines tatsächlichen Datums.
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:

Von: **leer**.

Bis: **leer**.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Letzter Tag eines jeden Monats“-Planung wird den Voll-Backups hinzugefügt, während die differentiellen Backups zur einmaligen Ausführung pro Woche und inkrementelle an Wochentagen geplant werden. Zu weiteren Details siehe die Beispiele über monatliche vollständige, wöchentliche differentielle und tägliche inkrementelle Backups sowie zu Bereinigung im Abschnitt Benutzerdefiniertes Backup-Schema (S. 51).

„Jahreszeiten“-Planung

Den Task an allen Werktagen während der nördlichen Herbst-Jahreszeit von 2009 und 2010 ausführen. Während eines Werktages wird der Task alle 6 Stunden von 0:00 (Mitternacht) bis 18:00 Uhr gestartet.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **September, Oktober, November**.
2. Am(Um): **<alle> <Werktage>**.
3. Alle: **6** Stunden.

   Von: **00:00 Uhr** bis: **18:00:00 Uhr**.
4. Wirksam:

   Von: **30.08.2009**. Tatsächlich wird der Task am ersten Werktag des Septembers gestartet. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2009 gestartet werden muss.

   Bis: **01.12.2010**. Tatsächlich wird der Task am letzten Werktag des Novembers enden. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2010 nicht fortgesetzt werden darf, nachdem der Herbst in der nördlichen Hemisphäre endet.

Mehrere monatliche Planungen für einen Task

In Fällen, in denen der Task an verschiedenen Tagen oder Wochen mit verschiedenen, vom Monat abhängigen Zeitintervallen ausgeführt werden muss, sollten Sie erwägen, jedem gewünschten Monat oder mehreren Monaten eine geeignete Planung zuzuweisen.

Angenommen, der Task tritt am 01.11.2009 in Kraft.

- Während des nördlichen Winters läuft der Task einmal um 22:00 Uhr an jedem Werktag.
- Während des nördlichen Frühlings und Herbstes läuft der Task alle 12 Stunden an allen Werktagen.
- Während des nördlichen Sommers läuft der Task an jedem 1. und 15. eines Monats um 22:00 Uhr.

Somit werden die folgenden drei Planungen dem Task hinzugefügt:

Erste Planung

1. Monate: **Dezember**, **Januar**, **Februar**.
2. Am(Um): **<Alle> <An allen Werktagen>.**
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:

   Von: **11/01/2009**.

   Bis: **nicht eingestellt**.

Zweite Planung

1. Monate: **März**, **April**, **Mai**, **September**, **Oktober**, **November**.
2. Am(Um): **<Alle> <An allen Werktagen>**.
3. Alle: **12 Stunden**
   Von: **00:00 Uhr** bis: **12:00 Uhr**.
4. Wirksam:
   Von: **11/01/2009**.
   Bis: **nicht eingestellt**.

Dritte Planung

1. Monate: **Juni**, **Juli**, **August**.
2. Tage: **1**, **15**.
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:
   Von: **11/01/2009**.
   Bis: **nicht eingestellt**.

4.4.4 Bei Ereignis in der Windows-Ereignisanzeige

Diese Art der Planung ist nur in Windows-Betriebssystemen wirksam.

Sie können einen Backup-Task so planen, dass er gestartet wird, wenn ein bestimmtes Windows-Ereignis in eine der Protokolllisten (Anwendungen, Sicherheit oder System) aufgenommen wird.

Angenommen, Sie wollen einen Backup-Plan aufstellen, der automatisch ein vollständiges Notfall-Backup Ihrer Daten durchführt, sobald Windows entdeckt, dass die Festplatte vor einem Ausfall steht.

Parameter

Protokollname

Spezifizieren Sie den Namen eines Protokolls. Wählen Sie den Namen einer Standard-Protokollliste (**Anwendung**, **Sicherheit** oder **System**) oder geben Sie den Namen einer Protokollliste ein – beispielsweise: **Microsoft Office Sitzungen**

Ereignisquelle

Spezifizieren Sie die Quelle des Ereignisses, welche typischerweise das Programm oder die Systemkomponente angibt, die das Ereignis verursachte – beispielsweise: **disk**

Ereignistyp

Geben Sie den Typ des Ereignisses an: **Fehler**, **Warnung**, **Informationen**, **Überprüfung erfolgreich** oder **Überprüfung fehlgeschlagen**.

Ereignis-Kennung:

Bezeichnet die Ereignis-Nummer, die üblicherweise die spezielle Art der Ereignisse unter Ereignissen derselben Quelle identifiziert.

So tritt z.B. ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **7** auf, wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, während ein **Fehler**-Ereignis mit

der Ereignisquelle **disk** und der Ereignis-Kennung **15** stattfindet, wenn eine Festplatte noch nicht zugriffsbereit ist.

Beispiele

„Fehlerhafte Blöcke"-Notfall-Backup

Treten ein oder mehrere fehlerhafte Blöcke plötzlich auf einer Festplatte auf, so deutet das üblicherweise auf einen baldigen Ausfall der Festplatte hin. Angenommen, Sie wollen einen Backup-Plan erstellen, der die Daten einer Festplatte sichert, sobald eine solche Situation eintritt:

Wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, nimmt es ein Ereignis mit der Ereignis-Quelle **disk** und der Ereignis-Kennung **7** in die Protokollliste **System** auf; der Typ des Ereignisses ist **Fehler**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **disk**
- **Ereignis-Typ**: **Fehler**
- **Ereignis-Kennung**: **7**

Wichtig: *Um sicherzustellen, dass ein solcher Task trotz Vorhandenseins der fehlerhaften Blöcke fertiggestellt wird, müssen Sie angeben, dass der Task diese ignoriert. Zur Umsetzung gehen Sie in den* ***Backup-Optionen*** *zum Unterpunkt* ***Fehlerbehandlung*** *und aktivieren das Kontrollkästchen* ***Fehlerhafte Sektoren ignorieren****.*

Vor-Update-Backup in Windows Vista

Angenommen Sie wollen einen Backup-Plan erstellen, der automatisch ein Backup des Systems durchführt – z.B. durch Sicherung der Partition, auf der Windows installiert ist – jedes Mal, wenn Windows davor steht, Updates zu installieren.

Nach dem Download eines oder mehrerer Updates und Planung der Installation nimmt Windows Vista ein Ereignis mit der Quelle **Microsoft-Windows-WindowsUpdateClient** und der Ereignis-Nummer **18** in die Protokollliste **System** auf; der Typ dieses Ereignisses ist **Informationen**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **Microsoft-Windows-WindowsUpdateClient**
- **Ereignis-Typ**: **Informationen**
- **Ereignis-Kennung**: **18**

Tipp: *Um einen vergleichbaren Backup-Plan für unter Windows XP laufende Maschinen aufzusetzen, ersetzen Sie den Text in* ***Ereignis-Quelle*** *mit* ***Windows Update Agent*** *und lassen Sie die übrigen Felder gleich.*

So können Sie Ereignisse in der Ereignisanzeige einsehen

So öffnen Sie eine Meldung in der Ereignisanzeige

1. Klicken Sie auf dem Desktop oder im **Start-**Menü mit der rechten Maustaste auf **Computer** und dann im Kontextmenü auf **Verwalten**.
2. Erweitern Sie in der Konsole **Computerverwaltung** den Zweig **System** und dann **Ereignisanzeige**.
3. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

***Hinweis:** Um die Sicherheitsprotokollliste öffnen zu können (**Sicherheit**), müssen Sie Mitglied der Gruppe „Administratoren" sein.*

So können Sie die Eigenschaften eines Ereignisses einsehen, inklusive seiner Quelle und Nummer (Ereigniskennung).

1. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

   ***Hinweis:** Um die Sicherheitsprotokollliste öffnen zu können (**Sicherheit**), müssen Sie Mitglied der Gruppe „Administratoren" sein.*

2. Klicken Sie im rechten Fensterbereich der Protokollliste auf den Namen des Ereignisses, dessen Eigenschaften Sie sehen wollen.
3. Im Dialogfenster **Eigenschaften** sehen Sie alle Informationen des Ereignisses, wie etwas seinen Ursprung im Feld **Quelle**, und seine Nummer, die im Feld **Ereignis-Kennung** angezeigt wird.

Sind Sie fertig, so klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

4.4.5 Bedingungen

Bedingungen erweitern den Scheduler mit mehr Flexibilität und ermöglichen es, Backup-Tasks abhängig von gewissen Bedingungen auszuführen. Sobald ein spezifiziertes Ereignis eintritt (siehe den Abschnitt 'Planung (S. 66)' zur Liste verfügbarer Ereignisse), überprüft der Scheduler die angegebene Bedingung und führt den Task aus, sofern die Bedingung zutrifft.

Bedingungen sind nur bei Verwendung des benutzerdefinierten Backup-Schemas (S. 51) verfügbar. Bedingungen können für vollständige, inkrementelle und differentielle Backups separat konfigurieren werden.

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option **Task-Startbedingungen** (S. 108) definiert. Dort können Sie angeben, wie wichtig die Bedingungen für die Backup-Strategie sind:

- Bedingungen sind zwingend – setzt die Ausführung des Backup-Tasks auf Wartestellung, bis alle Bedingungen zutreffen.
- Bedingungen sind wünschenswert, aber die Ausführung eines Backup-Tasks hat höhere Priorität – setzt den Task für das angegebene Zeitintervall auf Wartestellung. Wenn das Zeitintervall vergeht und die Bedingungen immer noch nicht zutreffen, führe den Task auf jeden Fall aus. Mit dieser Einstellung handhabt das Programm automatisch Situationen, wenn Bedingungen eine zu lange Zeit nicht zutreffen und eine weitere Verzögerung des Backups unerwünscht ist.
- Startzeit des Backup-Tasks ist relevant – überspringe den Backup-Tasks, wenn die Bedingungen zu dem Zeitpunkt, wenn der Task gestartet werden soll, nicht zutreffen. Ein Überspringen der Task-Ausführung macht Sinn, wenn Sie Daten ganz genau zur angegebenen Zeit sichern müssen, insbesondere, wenn die Ereignisse relativ häufig sind.

Mehrere Bedingungen hinzufügen

Sollten zwei oder mehr Bedingungen spezifiziert sein, dann wird das Backup nur starten, wenn alle davon erfüllt sind.

4.4.5.1 Benutzer ist untätig

Gilt für: Windows

„Benutzer ist untätig“ bedeutet, dass auf der verwalteten Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel:

Starte den Backup-Task auf der verwalteten Maschine täglich um 21:00 Uhr, möglichst, wenn der Benutzer untätig ist. Ist der Benutzer um 23 Uhr immer noch aktiv, starte den Task dennoch.

- Ereignis: **Täglich**, alle **1** Tage; einmal um: **09:00:00 PM**.
- Bedingung: **Benutzer ist untätig**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **2** Stunde(n).

Ergebnis:

(1) Wenn der Benutzer vor 21 Uhr untätig wird, startet der Backup-Task um 21 Uhr.

(2) Wenn der Benutzer zwischen 21 und 23 Uhr untätig wird, startet der Backup-Task sofort, nachdem der Benutzer untätig wurde.

(3) Wenn der Benutzer um 23 Uhr immer aktiv ist, startet der Backup-Task dennoch.

4.4.5.2 Host des Speicherorts verfügbar ist

Gilt für: Windows, Linux

„Host des Speicherorts ist verfügbar“ bedeutet, dass die Maschine, die das Ziel zum Speichern von Archiven auf einem Netzlaufwerk bereithält, verfügbar ist.

Beispiel:

Eine Datensicherung zu einem Netzwerk-Speicherort wird werktags um 21:00 Uhr durchgeführt. Wenn der Speicherort des Hosts zu dem Zeitpunkt nicht verfügbar ist (z.B. wegen Wartungsarbeiten), überspringe das Backup und warte bis zum nächsten Werktag, um den Task zu starten. Es wird angenommen, dass der Backup-Task besser überhaupt nicht gestartet werden soll, statt fehlzuschlagen.

- Ereignis: **Wöchentlich**, alle **1** Woche(n) an **<Werktagen>**; einmal um **21:00 Uhr**.
- Bedingung: **Host des Speicherorts verfügbar ist**
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und der Host des Speicherorts verfügbar ist, startet der Backup-Task zur rechten Zeit.

(2) Wenn es 21:00 Uhr wird, der Host im Augenblick aber nicht verfügbar ist, dann startet der Backup-Task am nächsten Werktag, sofern der Host des Speicherorts dann verfügbar ist.

(3) Wenn der Host des Speicherorts an Werktagen um 21:00 Uhr niemals verfügbar ist, startet auch der Task niemals.

4.4.5.3 Entspricht Zeitintervall

Gilt für: Windows, Linux

Beschränkt die Startzeit eines Backup-Tasks auf ein angegebenes Zeitintervall.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben netzwerkangebundenen Speicher zur Sicherung von Benutzerdaten und Servern. Der Arbeitstag startet um 8:00 und endet um 17:00 Uhr. Die Benutzerdaten sollen gesichert werden, sobald der User sich abmeldet, aber nicht vor 16:30 Uhr und nicht später als 22:00 Uhr. Die Firmen-Server werden jeden Tag um 23:00 Uhr per Backup gesichert. Daher sollten alle Daten der Benutzer vorzugsweise vor dieser Zeit gesichert werden, um Netzwerk-Bandbreite frei zu machen. Indem Sie das obere Limit auf 22:00 Uhr setzen, wird angenommen, dass die Sicherung der Benutzerdaten nicht länger als eine Stunde benötigt. Wenn ein Benutzer innerhalb des angegebenen Zeitintervalls noch angemeldet ist oder sich zu irgendeiner anderen Zeit abmeldet – sichere keine Benutzerdaten, d.h. überspringe die Task-Ausführung.

- Ereignis: **Beim Abmelden**, Der folgende Benutzer: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall** von **16:30 Uhr** bis **22:00 Uhr**.
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn sich der Benutzer zwischen 16:30 Uhr und 22:00 Uhr abmeldet, wird der Backup-Task unmittelbar nach der Abmeldung gestartet.

(2) Wenn sich der Benutzer zu einer anderen Zeit abmeldet, wird der Task übersprungen.

Was ist, wenn...

Was ist, wenn ein Task-Ausführung für einen bestimmten Zeitpunkt geplant ist und dieser außerhalb des spezifizierten Zeitintervalls liegt?

Ein Beispiel:

- Ereignis: **Täglich**, alle **1** Tage; einmal um **15:00 Uhr**.
- Bedingung: **Entspricht dem Zeitintervall** von **18:00 Uhr** bis **23:59:59 Uhr**.

In diesem Fall hängt die Antwort auf die Frage, ob und wann der Task ausgeführt wird, von den Task-Startbedingungen ab:

- Wenn die Task-Startbedingungen **Ausführung des Tasks übergehen** lauten, dann wird der Task niemals laufen.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** *deaktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 18:00 Uhr gestartet — dem Zeitpunkt, wenn die Bedingung erfüllt ist.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** mit z.B. einer Wartezeit von **1 Stunde** *aktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 16:00 Uhr gestartet — dem Zeitpunkt, zu dem die Warteperiode endet.

4.4.5.4 Benutzer ist abgemeldet

Gilt für: Windows

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis sich alle Benutzer auf der verwalteten Maschine von Windows abgemeldet haben.

Beispiel

Führe den Backup-Task um 20:00 Uhr am ersten und dritten Freitag eines jeden Monats aus, möglichst, wenn alle Benutzer abgemeldet sind. Sollte einer der Benutzer um 23:00 Uhr immer noch angemeldet sein, führe den Task dennoch aus.

- Ereignis: **Monatlich**, Monate: **<Alle>**; An: **<Erster>**, **<Dritter> <Freitag>**; einmalig um **20:00 Uhr**.
- Bedingung: **Benutzer sind abgemeldet**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **3** Stunde(n).

Ergebnis:

(1) Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, startet der Backup-Task um 20:00 Uhr.

(2) Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird der Backup-Task sofort ausgeführt, nachdem sich der Benutzer abgemeldet hat.

(3) Wenn ein Benutzer um 23:00 Uhr immer noch angemeldet ist, startet der Backup-Task dennoch.

4.4.5.5 Zeit seit letztem Backup

Gilt für: Windows, Linux

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis das angegebene Zeitintervall verstreicht, seit das letzte Backup erfolgreich fertiggestellt wurde.

Beispiel:

Den Backup-Task bei Systemstart ausführen, aber nur, wenn mehr als 12 Stunden seit dem letzten erfolgreichen Backup verstrichen sind.

- Ereignis: **Beim Start**, führt den Task beim Starten der Maschine aus.
- Bedingung: **Zeit seit dem letzten Backup**, Zeit seit dem letzten Backup: **12** Stunden.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn die Maschine neu gestartet wird, bevor seit Abschluss des letzten erfolgreichen Backup 12 Stunden verstrichen sind, dann wird der Scheduler warten, bis die 12 Stunden abgelaufen sind und dann den Task starten.

(2) Wenn die Maschine mindestens 12 Stunden nach Abschluss des letzten erfolgreichen Backups neu gestartet wird, dann wird der Backup-Task direkt ausgeführt.

(3) Wenn die Maschine niemals neu gestartet wird, wird auch der Task niemals ausgeführt. Sie können das Backup in der Ansicht **Backup-Pläne und Tasks** manuell starten, falls das nötig ist.

4.5 Replikation und Aufbewahrung von Backups

Bei Erstellung eines Backup-Plans (S. 38) spezifizieren Sie den primären Speicherort für die Backups. Zusätzlich können Sie Folgendes tun:

- Jedes Backup als 'Replikat' direkt nach seiner Erstellung zu einem zweiten Speicherort kopieren lassen.

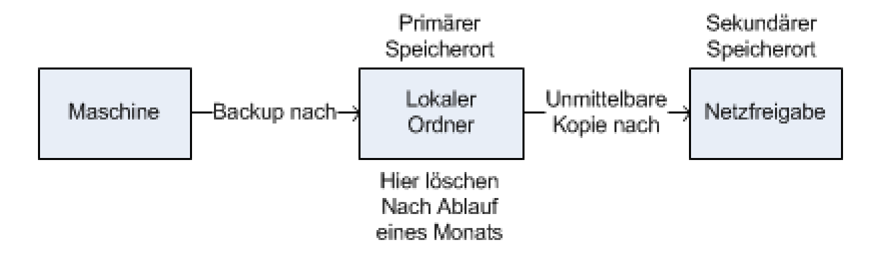
- Die Backups entsprechend der von Ihnen spezifizierten Aufbewahrungsregeln bewahren und sie dann entweder zu einem zweiten Speicherort zu verschieben oder sie zu löschen.

Auf ähnliche Weise können Sie Backups von einem zweiten Speicherort zu einem dritten kopieren oder verschieben (usw.). Es werden bis zu fünf aufeinanderfolgende Speicherorte unterstützt (den ersten eingeschlossen).

Hinweis: *Die Replikationsfunktion ersetzt und erweitert die Option **Dual Destination**, die in Acronis Backup & Recovery 10 verfügbar war.*

Beispiel: Sie erstellen ein Backup Ihrer Maschine in einen lokalen Ordner. Das Backup wird unmittelbar in einen Netzwerkordner kopiert. Das Backup wird im ursprünglichen lokalen Ordner nur für einen Monat gespeichert.

Das folgende Bild illustriert dieses Beispiel.



Einsatzszenarien

- **Verlässliches Desaster-Recovery** (S. 85)

  Speichern Sie Ihre Backups sowohl 'on-site' (zur sofortigen Wiederherstellung) wie auch 'off-site' (um die Backups vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen).
- **Nur die jüngsten Recovery-Punkte bewahren** (S. 86)

  Löschen Sie ältere Backups von einem schnellen Speicher gemäß den Aufbewahrungsregeln, um teuren Speicherplatz nicht übermäßig zu beanspruchen.
- **Acronis Cloud Backup verwenden, um Daten vor einem natürlichen Desaster zu schützen** (S. 86)

  Replizieren Sie Archive zum Cloud Storage, indem lediglich Änderungen an den Daten außerhalb der üblichen Arbeitsstunden übertragen werden.
- **Reduzierte Kosten bei der Speicherung von Backups**

  Speichern Sie Ihre Backups solange auf einem schnellen Speicher, wie es wahrscheinlich ist, dass Sie auf diese Daten zugreifen müssen. Verschieben Sie sie danach auf einen Speicher mit niedrigeren Kosten, um Sie dort für einen längeren Zeitraum aufbewahren zu können. Das ermöglicht Ihnen auch, gesetzliche Bestimmungen zur Datenaufbewahrung einzuhalten.

Replikation und Aufbewahrung in Backup-Schemata

Die nachfolgende Tabelle zeigt die Verfügbarkeit von Replikation und Aufbewahrungsregeln in verschiedenen Backup-Schemata.

Backup-Schema	Kann Backups kopieren	Kann Backups verschieben	Kann Backups löschen
Manueller Start (S. 56)	Ja	Nein	Nein
Einfach (S. 47)	Ja	Ja	Ja
GVS (Großvater-Vater-Sohn) (S. 48)	Ja	Nein	Ja
Türme von Hanoi (S. 54)	Ja	Nein	Ja

Benutzerdefiniert (S. 51)	Ja	Ja	Ja
Initial Seeding (S. 57)	Nein	Nein	Nein

Anmerkungen:

- Eine Konfiguration, bei der Backups vom selben Speicherort gleichermaßen kopiert und verschoben werden, ist nicht möglich.
- In Kombination mit der Option Vereinfachte Benennung von Backup-Dateien (S. 61) stehen weder Replikation noch Aufbewahrungsregeln zur Verfügung.

4.5.1 Unterstützte Speicherorte

Sie können ein Backup *von* jedem der nachfolgenden Speicherorte aus kopieren oder verschieben:

- Ein lokaler Ordner auf einem fest eingebauten Laufwerk
- Netzwerkordner
- FTP- oder SFTP-Server
- Acronis Secure Zone

Sie können ein Backup *zu* jedem der nachfolgenden Speicherorte kopieren oder verschieben:

- Ein lokaler Ordner auf einem fest eingebauten Laufwerk
- Netzwerkordner
- FTP- oder SFTP-Server
- Acronis Cloud Storage
- Ein Wechsellaufwerk (S. 170), welches im Modus **Eingebautes Laufwerk** verwendet wird. (Sie wählen beim Erstellen eines Backup-Plans den Wechsellaufwerkmodus.)

Backups, die zu einem nächsten Speicherort kopiert oder verschoben wurden, sind unabhängig von den Backups, die auf dem ursprünglichen Speicherort verbleiben (und umgekehrt). Sie können Daten von jedem dieser Backups wiederherstellen, ohne Zugriff auf andere Speicherorte.

Einschränkungen

- Kopieren oder Verschieben von Backups *auf und von* optischen Laufwerken (CD-, DVD-, Blu-ray-Medien) wird nicht unterstützt.
- Das Kopieren oder Verschieben von Backups *zu und von* Wechsellaufwerken, die im Modus **Wechselmedium** verwendet werden, wird nicht unterstützt.
- Der Acronis Cloud Storage kann nur der finale Speicherort sein. Nachfolgendes Kopieren oder Verschieben von Backups *von* dort aus ist nicht möglich.
- Sie können denselben Speicherort nicht mehr als einmal spezifizieren. Sie können ein Backup beispielsweise nicht von einem Ordner zu einem anderen verschieben – und dann wieder zurück zum ursprünglichen Ordner.

4.5.2 Replikation von Backups einrichten

Sie können eine Replikation von Backups konfigurieren, wenn Sie einen Backup-Plan erstellen (S. 38).

- Aktivieren Sie zur Einrichtung einer Replikation, die vom primären Speicherort ausgeht, das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren**.
- Aktivieren Sie zur Einrichtung einer Replikation, die vom zweiten oder einen weiteren Speicherort ausgeht, das Kontrollkästchen **Backups, sobald Sie an diesem Speicherort erscheinen, zu einem anderen Speicherort replizieren**.

Bestimmen Sie anschließend den Speicherort, wohin die Backups repliziert werden.

Sofern vom Backup-Schema zugelassen, können Sie zusätzlich festlegen, wann die Backups auf jedem dieser Speicherorte automatisch gelöscht werden sollen.

Ein Backup wird zum jeweils nächsten Speicherort repliziert, sobald es im vorherigen Speicherort erscheint. Falls frühere Backups nicht repliziert wurden (weil beispielsweise die Netzwerkverbindung verloren ging), wird die Software auch alle Backups replizieren, die nach der letzten erfolgreichen Replikation erschienen sind.

4.5.3 Aufbewahrung von Backups einrichten

Aufbewahrungsregeln können bei Erstellung eines Backup-Plans (S. 38) konfiguriert werden. Welche Aufbewahrungsregeln verfügbar sind, hängt vom gewählten Backup-Schema ab.

Das Anwenden von Aufbewahrungsregeln kann durch die Option **Inaktivitätszeit für Replikation/Bereinigung** (S. 85) eingeschränkt werden.

Schema 'Einfach'

Jedes Backup wird solange aufbewahrt, bis sein Alter einen von Ihnen spezifizierten Grenzwert überschreitet. Danach wird es entweder gelöscht oder verschoben.

So konfigurieren Sie, dass die Backups gelöscht werden:

- Wählen Sie in den **Aufbewahrungsregeln** die Option **Lösche Backups älter als...** und spezifizieren Sie dann die Aufbewahrungsdauer.

So konfigurieren Sie, dass die Backups verschoben werden:

- Wählen Sie in den **Aufbewahrungsregeln** die Option **Verschiebe Backups älter als...** und spezifizieren Sie dann die Aufbewahrungsdauer. Spezifizieren Sie unter **Ziel für Replikation/Verschieben der Backups** den entsprechenden Speicherort.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Für den zweiten und weitere Speicherorte bedeutet die Backup-Erstellung, dass ein Backup vom vorherigen Speicherort ausgehend dorthin kopiert oder verschoben wird.

Schema 'Großvater-Vater-Sohn' (GVS)

Backups jeden Typs (täglich, wöchentlich, monatlich) werden für die unter '**Backups behalten**' definierte Aufbewahrungsdauer einbehalten und dann gelöscht.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Sie werden nacheinander auf den primären, sekundären sowie alle nachfolgenden Speicherorte angewendet.

Schema 'Türme von Hanoi'

Jedes Backup wird basierend auf seinem Level (S. 54) einbehalten und dann gelöscht. Wie viele Level das sind, spezifizieren Sie unter **Zahl der Level**.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Sie werden nacheinander auf den primären, sekundären sowie alle nachfolgenden Speicherorte angewendet.

Benutzerdefiniertes Schema

Jedes Backup wird solange aufbewahrt, bis die von Ihnen spezifizierten Regeln zutreffen. Danach wird es entweder gelöscht oder verschoben.

So konfigurieren Sie, dass die Backups gelöscht werden:

- Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**. Spezifizieren Sie im Fenster **Aufbewahrungsregeln** (S. 83) die entsprechenden Regeln und wählen Sie dann **Wenn die spezifizierten Bedingungen zutreffen: Die ältesten Backups löschen**.
- Spezifizieren Sie unter **Aufbewahrungsregeln anwenden**, wann die Regeln ausgeführt werden sollen.

So konfigurieren Sie, dass die Backups verschoben werden:

- Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**. Spezifizieren Sie im Fenster **Aufbewahrungsregeln** (S. 83) die entsprechenden Regeln und wählen Sie dann **Wenn die spezifizierten Bedingungen zutreffen: Die ältesten Backups an einen anderen Speicherort verschieben**. Klicken Sie auf **OK** und spezifizieren Sie dann unter **Ziel für Replikation/Verschieben der Backups** den entsprechenden Speicherort.
- Spezifizieren Sie unter **Aufbewahrungsregeln anwenden**, wann die Regeln ausgeführt werden sollen.

Sie können wählen, ob die Aufbewahrungsregeln vor der Backup-Erstellung, danach, auf Planung oder gemäß einer Kombination dieser Optionen angewendet werden sollen. Für den zweiten und weitere Speicherorte bedeutet die Backup-Erstellung, dass ein Backup vom vorherigen Speicherort ausgehend dorthin kopiert oder verschoben wird.

4.5.4 Aufbewahrungsregeln für das benutzerdefinierte Schema

Sie können im Fenster **Aufbewahrungsregeln** wählen, wie lange Backups an einem Speicherort vorgehalten werden sollen und ob diese anschließend gelöscht oder verschoben werden sollen.

Die Regeln werden auf alle diejenigen Backups angewendet, die von dieser *speziellen Maschine* gemacht wurden und in diesem *speziellen Speicherort* durch diesen *speziellen Backup-Plan* abgelegt wurden. Ein solcher Satz von Backups wird in Acronis Backup auch *Archiv* genannt.

So richten Sie Aufbewahrungsregeln für Backups ein:

1. Spezifizieren Sie eine der folgenden Möglichkeiten (Option (a) und (b) schließen sich gegenseitig aus):
   a. **Backups älter als...** und/oder **Archiv größer als...**.

      Ein Backup wird solange gespeichert, bis die spezifizierte Bedingung (oder beide Bedingungen) eintreffen.

      Beispiel:

      Backups älter als 5 Tage

      Archiv größer als 100 GB

      Mit diesen Einstellungen wird ein Backup solange gespeichert, bis es älter als 5 Tage ist *und* die Größe des Archivs, indem es enthalten ist, 100 GB übersteigt.

   b. **Anzahl der Backups im Archiv überschreitet...**

      Fall die Anzahl an Backups den spezifizierten Wert überschreitet, werden eins oder mehrere der ältesten Backups verschoben oder gelöscht. Die kleinste Einstellung ist 1.

2. Bestimmen Sie, ob die Backups gelöscht oder zu einem anderen Speicherort verschoben werden sollen, sofern die angegebenen Bedingungen zutreffen.

   Sie können den Speicherort angegeben, zu dem die Backups verschoben werden sollen und nach Klicken auf **OK** auch für diesen Speicherort Aufbewahrungsregeln einstellen.

Das letzte Backup in dem Archiv löschen

Die Aufbewahrungsregeln sind wirksam, wenn das Archiv mehr als ein Backup enthält. Das bedeutet, dass das letzte Backup im Archiv erhalten bleibt, selbst wenn dabei die Verletzung einer Aufbewahrungsregel entdeckt wird. Versuchen Sie nicht, das einzige vorhandene Backup zu löschen, indem Sie die Aufbewahrungsregeln *vor* dem Backup anwenden. Dies wird nicht funktionieren. Verwenden Sie die alternative Einstellung **Archiv bereinigen** –> **Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist** (S. 51); beachten Sie dabei aber das Risiko, möglicherweise das letzte Backup verlieren zu können.

Backups mit Abhängigkeiten löschen oder verschieben

Klicken Sie zum Zugriff auf diese Einstellungen im Fenster **Aufbewahrungsregeln** auf **Erweiterte Einstellungen anzeigen**.

Aufbewahrungsregeln setzen das Löschen einiger Backups und die Bewahrung anderer voraus. Aber was, wenn das Archiv inkrementelle und differentielle Backups enthält, die voneinander und von dem Voll-Backup abhängen, auf dem diese basieren? Sie können kein veraltetes Voll-Backup löschen und sozusagen seine inkrementellen „Kinder“ behalten.

Wenn das Löschen oder Verschieben eines Backups andere Backups beeinflusst, wird eine der folgenden Regeln angewendet:

- **Backup bewahren, bis alle abhängigen Backups gelöscht (verschoben) werden**

  Das veraltete Backup (mit dem Icon gekennzeichnet) wird solange bewahrt, bis alle auf ihm beruhenden Backups ebenfalls veraltet sind. Dann wird die gesamte Kette während der regulären Bereinigung sofort gelöscht. Falls Sie festgelegt haben, dass die veralteten Backups zum nächsten Speicherort verschoben werden sollen, dann wird das Backup ohne Verzögerung dorthin kopiert. Nur seine Löschung vom aktuellen Speicherort wird aufgeschoben.

  Dieser Modus hilft, die potentiell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Die Archivgröße, das Backup-Alter oder die Backup-Anzahl kann daher die von Ihnen spezifizierten Werte überschreiten.

  Dieser Modus ist nicht für den Acronis Cloud Storage verfügbar, wenn Sie Backups dorthin kopieren oder verschieben. Im Cloud Storage sind alle Backup inkrementell, mit Ausnahme des ersten Backups eines Archivs, welches immer vollständig ist. Diese Kette kann nicht komplett gelöscht werden, weil das aktuellste Backup immer aufbewahrt werden muss.

- **Diese Backups konsolidieren**

  Die Software wird das Backup, das einer Löschung oder Verschiebung unterworfen ist, mit dem nächsten abhängigen Backup konsolidieren. Zum Beispiel erfordern die Aufbewahrungsregeln, ein Voll-Backup zu löschen, das nachfolgende inkrementelle Backup jedoch zu bewahren. Die Backups werden zu einem einzelnen Voll-Backup kombiniert, welches den Zeitstempel des inkrementellen Backups erhält. Wenn ein inkrementelles oder differentielles Backup aus der Mitte einer Kette gelöscht wird, wird der resultierende Backup-Typ inkrementell.

  Dieser Modus stellt sicher, dass nach jeder Bereinigung die Archivgröße, sowie Alter und Anzahl der Backups innerhalb der von Ihnen spezifizierten Grenzen liegen. Die Konsolidierung kann jedoch viel Zeit und Systemressourcen in Anspruch nehmen. Sie benötigen zusätzlichen Platz im Depot für temporäre Daten, die während der Konsolidierung erstellt werden.

  Dieser Modus ist nicht verfügbar, falls Sie die Regel **Archiv größer als** für jeden Archiv-Speicherort (Acronis Cloud Storage ausgenommen) aktiviert haben.

  Das sollten Sie über Konsolidierung wissen

Machen Sie sich bewusst, dass Konsolidierung nur eine Methode, aber keine Alternative zum Löschen ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im beibehaltenen inkrementellen oder differentiellen Backup fehlten.

4.5.5 Inaktivitätszeit für Replikation/Bereinigung

Diese Option ist nur wirksam, wenn Sie für Backups entweder Replikation oder Aufbewahrungsregeln (S. 79) einrichten.

Die Option definiert einen Zeitraum, in dem der Start einer Replikation oder die Anwendung von Aufbewahrungsregeln nicht erlaubt ist. Diese Aktionen werden daher dann ausgeführt, wenn die Inaktivitätszeit beendet ist und sofern die Maschine zu diesem Zeitpunkt eingeschaltet ist. Aktionen, die vor dem Inaktivitätszeitraum gestartet wurden, werden ohne Unterbrechung fortgesetzt.

Die Inaktivitätszeit betrifft alle Speicherorte, den primären eingeschlossen.

Voreinstellung ist: **Deaktiviert.**

Aktivieren Sie zur Spezifikation der Inaktivitätszeit das Kontrollkästchen **Replikation/Bereinigung in folgender Zeit nicht starten** und wählen Sie dann die Tage und den entsprechenden Zeitraum.

Anwendungsbeispiele

Sie können diese Option auf Wunsch verwenden, um den eigentlichen Backup-Prozess von der Replikation oder Bereinigung zu separieren. Nehmen Sie beispielsweise an, dass Sie Maschinen lokal sowie tagsüber sichern und die entsprechenden Backups dann zu einem Netzwerkordner replizieren. Stellen Sie die Inaktivitätszeit so ein, dass sie die reguläre Arbeitszeit enthält. Die Replikation wird daraufhin nach diesen Arbeitstunden gemacht, wenn auch die Netzwerklast geringer ist.

4.5.6 Anwendungsbeispiele

In diesem Abschnitt finden Sie Beispiele dafür, wie Sie Replikate von Backups erstellen und Aufbewahrungsregeln für diese konfigurieren können.

4.5.6.1 Beispiel 1: Backups zu einem Netzwerkordner replizieren

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine manuell per Voll-Backup sichern.
- Sie möchten die Backups in der Acronis Secure Zone (S. 166) dieser Maschine speichern.
- Sie möchten eine Kopie der Backups in einem Netzwerkordner speichern.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem Schema **Manueller Start**. Spezifizieren Sie bei Erstellung des Backup-Plans die Acronis Secure Zone im Feld **Speicherort**, wählen Sie **Vollständig** im Feld **Backup-Typ**, aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** – und spezifizieren Sie dann den Netzwerkordner im Feld **2. Speicherort**.

Ergebnis:

- Sie können die Volumes oder Dateien der Maschine von einem sofort verfügbaren, lokalen Backup wiederherstellen, welches in einem speziellen Bereich auf dem Festplattenlaufwerk gespeichert wird.
- Sie können die Maschine aber auch aus dem Netzwerkordner wiederherstellen, falls das Festplattenlaufwerk der Maschine ausfallen sollte.

4.5.6.2 Beispiel 2: Alter und Gesamtgröße gespeicherter Backups begrenzen

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem wöchentlichen Voll-Backup sichern.
- Sie möchten alle Backups aufbewahren, die jünger als ein Monat sind.
- Solange die Gesamtgröße aller Backups unterhalb von 200 GB bleibt, möchten Sie zudem auch noch ältere Backups behalten.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem **Benutzerdefinierten Schema**. Spezifizieren Sie bei Erstellung des Backup-Plans eine wöchentliche Planung für die Voll-Backups. Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**.

Klicken Sie auf **Aufbewahrungsregeln**, aktivieren Sie die Kontrollkästchen **Backups älter als** sowie **Archiv größer als** und spezifizieren Sie dann die entsprechenden Werte, nämlich **1 Monat** und **200 GB**. Wählen Sie unter **Wenn die spezifizierten Bedingungen zutreffen** die Einstellung **Älteste Backups löschen**.

Klicken Sie auf **OK**. Aktivieren Sie unter **Aufbewahrungsregeln anwenden** das Kontrollkästchen **Nach dem Backup**.

Ergebnis:

- Backups, die jünger als ein Monat sind, werden aufbewahrt – unabhängig von ihrer Gesamtgröße.
- Backups, die älter als ein Monat sind, werden nur dann aufbewahrt, wenn die Gesamtgröße aller Backups (ältere plus jüngere) nicht die 200 GB-Grenze überschreitet. Anderenfalls löscht die Software einige oder alle der älteren Backups, mit dem ältesten beginnend.

4.5.6.3 Beispiel 3: Replikation von Backups zum Cloud Storage

Dieses Beispiel geht davon aus, dass Sie ein aktiviertes (S. 287) Cloud Backup-Abonnement (S. 271) *für die Maschine haben, die Sie per Backup sichern.*

Das folgende Szenario nimmt an, dass die Datenmenge für das Backup relativ klein ist. Informationen zu größeren Backups finden Sie später in diesem Abschnitt unter 'Replikation größerer Datenmengen zum Cloud Storage'.

Betrachten Sie folgendes Szenario:

- Sie erstellen gelegentliche Backups Ihrer Maschine in einen lokalen Ordner.
- Sie möchten eine Kopie des resultierenden Archivs extern (offsite) im Acronis Cloud Backup Storage aufbewahren.
- Sie möchten, unabhängig vom Startzeitpunkt des Backups, dass die Replikation außerhalb der üblichen Arbeitszeiten stattfindet, wenn die Belastung der Internetverbindung niedriger ist.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem gewünschten Backup-Schema. Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** einen lokalen Ordner. Aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** und spezifizieren Sie dann im Feld **2. Speicherort** den Cloud Storage.

Gehen Sie in den **Backup-Optionen** zum Element **Inaktivitätszeit für Replikation/Bereinigung** (S. 85) und spezifizieren Sie die gängigen Arbeitsstunden (beispielsweise Montag bis Freitag von 8:00 bis 17:00 Uhr).

Ergebnis:

- Die Daten werden nach dem Start des Backup-Plans in den lokalen Ordner gesichert.
- Sollte das Backup außerhalb der definierten Arbeitsstunden abgeschlossen werden, dann wird die Replikation sofort gestartet. Anderenfalls wird die Replikation bis zum Ende der Arbeitsstunden verschoben.

Hinweis: *Im* Cloud *Storage sind das zweite und alle weiteren Backups eines Archivs immer inkrementell, egal welchen Typ sie am ursprünglichen Speicherort haben. Dadurch wird der Storage-Speicherplatz Ihres* Cloud *Backup-Abonnements effizient genutzt.*

Replikation größerer Datenmengen zum Cloud Storage

Falls Sie planen, Backups mit Daten von 100 GB und mehr zu erstellen, können Sie das erste Backup für den Cloud Storage auf einer physikalischen Festplatte an uns senden. Diese Option wird Ihnen über den Initial Seeding Service (S. 275) bereitgestellt, den Sie als Ergänzung zu Ihrem Cloud Backup-Abonnement erwerben können.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Bei allen nachfolgenden Backups werden nur noch Änderungen an den ursprünglichen Daten zum Cloud Storage gesendet, sodass der Netzwerkdatenverkehr nicht zu stark beeinflusst wird.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem Schema **Initial Seeding**. Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** einen lokalen Ordner. Dies kann ein Ordner auf der zu versendenden Festplatte sein. Weitere Details finden Sie unter 'Wie wird Initial Seeding ausgeführt? (S. 276)'.

Bearbeiten Sie den Backup-Plan, nachdem die Festplatte versendet und der Auftragsstatus auf **Der Upload der Daten wurde abgeschlossen** eingestellt wurde. Ändern Sie das Backup-Schema, das Ziel und die Replikationseinstellungen so, wie zuvor in diesem Abschnitt beschrieben.

Der aktualisierte Backup-Plan erstellt Backups, die außerhalb der üblichen Arbeitszeiten zum Cloud Storage repliziert werden.

4.6 So deaktivieren Sie die Backup-Katalogisierung

Durch die Katalogisierung eines Backups werden dessen Inhalte direkt nach seiner Erstellung dem Datenkatalog hinzugefügt.Dies kann ein zeitaufwendiges Verfahren sein. Daher möchten Sie möglicherweise die Katalogisierung auf einer verwalteten Maschine deaktivieren. Gehen Sie dafür zu **Optionen** –> **Maschinen-Optionen** und konfigurieren Sie die Option **Backup-Katalogisierung**.

4.7 Standardoptionen für Backup

Jeder Acronis Agent hat eigene Standardoptionen für Backups. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Backup-Plans können Sie entweder eine Standardoption verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Plan gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Backup-Pläne verwendet.

Um die Standardoptionen für Backups einsehen und verändern zu können, verbinden Sie die Konsole mit der verwalteten Maschine und wählen Sie dort aus dem Hauptmenü die Befehle **Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup**.

Verfügbarkeit der Backup-Optionen

Art und Umfang der verfügbaren Backup-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent arbeitet (Linux, bootfähige Medien)
- Dem Datentyp, der gesichert wird (Laufwerke, Dateien)
- Dem Backup-Ziel (Netzwerkpfad oder lokales Laufwerk)
- Dem Backup-Schema (manueller Start oder nach Planung)

Die nachfolgende Tabelle fasst die Verfügbarkeit der Backup-Optionen zusammen:

	Agent für Windows		**Bootfähiges Medium (Linux-basiert oder PE-basiert)**	
	Laufwerk-Backup	**Datei-Backup**	**Laufwerk-Backup**	**Datei-Backup**
Erweiterte Einstellungen (S. 89):				
Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen	Ziel: Wechselmedium	Ziel: Wechselmedium	Ziel: Wechselmedium	Ziel: Wechselmedium
Archivattribut zurücksetzen	-	+	-	+
Nach Abschluss des Backups die Maschine automatisch neu starten	-	-	+	+
Schutz des Archivs (S. 90) (Kennwort und Verschlüsselung)	+	+	+	+
Backup-Katalogisierung (S. 91)	+	+	-	-
Backup-Performance:				
Backup-Priorität (S. 92)	+	+	-	-
Schreibgeschwindigkeit auf Laufwerk (S. 92)	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk
Netzwerkverbindungsgeschwindigkeit (S. 93)	Ziel: Netzwerkfreigabe	Ziel: Netzwerkfreigabe	Ziel: Netzwerkfreigabe	Ziel: Netzwerkfreigabe
Backup-Aufteilung (S. 93)	+	+	+	+
Komprimierungsgrad (S. 94)	+	+	+	+
Desaster-Recovery-Plan (S. 95)	+	+	-	-
E-Mail-Benachrichtigungen (S. 96)	+	+	-	-
Fehlerbehandlung (S. 97):				
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)	+	+	+	+
Bei Fehler erneut versuchen	+	+	+	+

	Agent für Windows		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Backup	Datei-Backup	Laufwerk-Backup	Datei-Backup
Fehlerhafte Sektoren ignorieren	+	+	+	+
Ereignisverfolgung:				
Ereignisanzeige von Windows (S. 99)	+	+	-	-
SNMP (S. 98)	+	+	-	-
Schnelles inkrementelles/differentielles Backup (S. 99)	+	-	+	-
Snapshot für Backup auf Dateiebene (S. 99)	-	+	-	-
Sicherheit auf Dateiebene (S. 100):				
Dateisicherheitseinstellungen in Archiven bewahren	-	+	-	-
Verschlüsselte Dateien in Archiven unverschlüsselt speichern	-	+	-	-
Medienkomponenten (S. 101)	Ziel: Wechselmedium	Ziel: Wechselmedium	-	-
Mount-Punkte (S. 101)	-	+	-	-
Multi-Volume-Snapshot (S. 102)	+	+	-	-
Vor-/Nach-Befehle für das Backup (S. 103)	+	+	nur PE	nur PE
Befehle vor/nach der Datenerfassung (S. 104)	+	+	-	-
Inaktivitätszeit für Replikation/Bereinigung (S. 85)	+	+	-	-
Sektor-für-Sektor-Backup (S. 107)	+	-	+	-
Task-Fehlerbehandlung (S. 107)	+	+	-	-
Task-Startbedingungen (S. 108)	+	+	-	-
Volume Shadow Copy Service (S. 109)	+	+	-	-

4.7.1 Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Backup durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen

Diese Option ist nur beim Backup auf Wechselmedien wirksam.

Diese Option definiert, ob die Meldung **Legen Sie das erste Medium ein** erscheint, wenn Sie ein Wechselmedium zum Backup benutzen.

Voreinstellung ist: **Deaktiviert**.

Bei eingeschalteter Option ist es unmöglich, ein Backup auf ein Wechselmedium auszuführen, wenn der Benutzer nicht anwesend ist, weil das Programm auf eine Bestätigung dieser Meldung wartet. Deshalb sollten Sie diese Meldung ausschalten, wenn ein geplanter Task eine Sicherung auf ein Wechselmedium vorsieht. Mit dieser Einstellung kann der Task unbeaufsichtigt erfolgen, wenn ein Wechselmedium beim Start gefunden wird (z.B. eine CD-R/W).

Archivattribut zurücksetzen

Diese Option ist nur für Backups auf Dateiebene unter Windows-Betriebssystemen und beim Arbeiten nach dem Start vom Boot-Medium wirksam.

Voreinstellung ist: **Deaktiviert**.

Im Betriebssystem Windows hat jede Datei ein Attribut **Datei kann archiviert werden**, das über **Datei** –> **Eigenschaften** –> **Allgemein** –> **Erweitert** –> **Archiv- und Indexattribute** verfügbar wird. Dieses Attribut, auch Archiv-Bit genannt, wird durch das Betriebssystem jedes Mal gesetzt, wenn die Datei verändert wurde, und kann durch Backup-Anwendungen zurückgesetzt werden, wenn die Datei in ein Backup auf Dateiebene eingeschlossen wird. Das Archivattribut wird von vielen Anwendungen verwendet, z.B. Datenbanken.

Wenn das Kontrollkästchen **Archivattribut zurücksetzen** aktiviert ist, wird Acronis Backup das Archivattribut aller im Backup enthaltenen Dateien zurückzusetzen. Acronis Backup selbst nutzt das Archiv-Bit aber nicht. Bei Ausführung eines inkrementellen oder differentiellen Backups wird die Änderung einer Datei anhand der Änderung der Dateigröße und von Tag bzw. Zeitpunkt der letzten Speicherung ermittelt.

Nach Abschluss des Backups die Maschine automatisch neu starten

Diese Option ist nur verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Voreinstellung ist: **Deaktiviert**.

Wenn die Option eingeschaltet ist, wird Acronis Backup die Maschine neu starten, nachdem der Backup-Prozess vollendet ist.

Wenn die Maschine standardmäßig z.B. von einer Festplatte bootet und Sie dieses Kontrollkästchen aktivieren, wird unmittelbar nach Abschluss eines Backups durch den bootfähigen Agenten die Maschine neu gestartet werden und das Betriebssystem booten.

4.7.2 Schutz des Archivs

Diese Option ist für Windows-, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für Disk-Backups und Backups auf Dateiebene.

Diese Option definiert, ob das Archiv per Kennwort geschützt und der Inhalt des Archivs verschlüsselt werden soll.

Diese Option ist nicht verfügbar, wenn das Archiv bereits Backups enthält. Diese Option kann beispielsweise nicht verfügbar sein:

- Wenn Sie ein bereits existierendes Archiv als Ziel für einen Backup-Plan spezifizieren.

- Wenn Sie einen Backup-Plan bearbeiten, der bereits zu einem Backup geführt hat.

Voreinstellung ist: **Deaktiviert.**

So schützen Sie ein Archiv vor unberechtigtem Zugriff

1. Aktivieren Sie das Kontrollkästchen **Kennwort für das Archiv einrichten**.
2. Tragen Sie im Eingabefeld **Kennwort** ein Kennwort ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Wählen Sie eine der nachfolgenden Varianten:
   - **Nicht verschlüsseln** – das Archiv wird nur mit dem Kennwort geschützt.
   - **AES 128** – das Archiv wird mit Hilfe des Advanced Encryption Standard-Verfahrens (AES) und einer Tiefe von 128-Bit verschlüsselt.
   - **AES 192** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einer Tiefe von 192-Bit verschlüsselt.
   - **AES 256** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einer Tiefe von 256-Bit verschlüsselt.
5. Klicken Sie auf **OK**.

Der kryptografische Algorithmus AES arbeitet im Cipher Block Chaining Mode (CBC) und benutzt einen zufällig erstellten Schlüssel mit der benutzerdefinierten Größe von 128-, 192- oder 256-Bit. Je größer die Schlüsselgröße, desto länger wird das Programm für die Verschlüsselung brauchen, aber desto sicherer sind auch die Daten.

Der Kodierungsschlüssel ist dann mit AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert des Kennworts als Schlüssel dient. Das Kennwort selbst wird nirgendwo auf dem Laufwerk oder in der Backup-Datei gespeichert, der Kennwort-Hash dient nur der Verifikation. Mit dieser zweistufigen Methode sind die gesicherten Daten vor unberechtigten Zugriff geschützt – ein verlorenes Kennwort kann daher jedoch auch nicht wiederhergestellt werden.

4.7.3 Backup-Katalogisierung

Beim Katalogisieren eines Backups werden dessen Inhalte zum Datenkatalog hinzugefügt. Durch Verwendung des Datenkatalogs können Sie benötigte Daten leicht finden und für eine Recovery-Aktion auswählen.

Die Option **Backup-Katalogisierung** spezifiziert, ob mit dem Backup direkt nach seiner Erstellung eine vollständige oder schnelle Katalogisierung durchgeführt wird.

Diese Option ist nur wirksam, falls die Backup-Katalogisierung auf der gesicherten Maschine oder auf dem Storage Node aktiviert ist.

Voreinstellung ist: **Vollständige Katalogisierung.**

Falls Sie **Vollständige Katalogisierung** wählen, werden die Backup-Inhalt mit dem höchstmöglichen Detail-Level katalogisiert. Das bedeutet, dass folgende Daten im Katalog angezeigt werden:

- Bei Laufwerk-Backups – Laufwerke, Volumes, Dateien und Ordner.
- Bei Datei-basierten Backups – Dateien und Ordner.

Sie können die **Schnelle Katalogisierung** wählen, falls die vollständige Katalogisierung die Performance der verwalteten Maschine zu stark beeinflusst oder das Fenster für die Backup-Erstellung zu eng ist. Folgende Daten werden im Katalog angezeigt:

- Bei Laufwerk-Backups – nur Laufwerke und Volumes.

- Bei Datei-basierten Backups – nichts.

Um dem Katalog die vollständigen Inhalte bereits existierender Backups hinzuzufügen, können Sie die vollständige Katalogisierung bei Bedarf auch manuell starten.

Weitere Informationen zur Verwendung dieser Funktion finden Sie im Abschnitt 'Datenkatalog (S. 116)'.

4.7.4 Backup-Performance

Benutzen Sie diese Gruppe der Optionen, um die Nutzung der Netzwerk- und der System-Ressourcen zu steuern.

Die Optionen zur Steuerung der Performance haben mehr oder weniger spürbare Auswirkungen auf die Geschwindigkeit des Backups. Die Wirkung hängt von den Systemkonfigurationen und den physikalischen Eigenschaften der Geräte ab, die beim Backup als Quelle oder Ziel benutzt werden.

4.7.4.1 Backup-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Ausmaß der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Backup-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der Backup-Priorität kann den Backup-Prozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren (wie etwa der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk).

Voreinstellung ist: **Niedrig.**

So spezifizieren Sie die Priorität des Backup-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Backup-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Backup-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Backup-Prozesses und zieht Ressourcen von anderen Prozessen ab.

4.7.4.2 Schreibgeschwindigkeit der Festplatte

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn eine interne (feste) Festplatte der Maschine als Backup-Ziel für das laufende Backup gewählt wurde.

Ein laufendes Backup auf einer internen Festplatte (z.B. in der Acronis Secure Zone) kann die Performance anderer Programme beeinträchtigen, weil eine große Datenmenge auf die Festplatte geschrieben werden muss. Sie können den Festplattengebrauch durch das Backup-Verfahren auf einen gewünschten Grad begrenzen.

Voreinstellung ist: **Maximum.**

So stellen Sie die gewünschte Schreibgeschwindigkeit für das Backup ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Schreibgeschwindigkeit in Prozent bezogen auf die maximale Geschwindigkeit der Zielfestplatte** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Schreibgeschwindigkeit in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

4.7.4.3 Netzwerkverbindungsgeschwindigkeit

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn ein Speicherort im Netzwerk (freigegebenes Netzlaufwerk, verwaltetes Depot oder FTP-/SFTP-Server) als Ziel für das Backup gewählt wurde.

Die Option definiert den Betrag der Bandbreite für die Netzwerkverbindung, die zum Übertragen der gesicherten Daten zugeteilt wird.

Als Standard ist dieser Wert auf das Maximum gesetzt, d.h. die Software benutzt die gesamte Netzwerkbandbreite zum Übertragen der gesicherten Daten, die sie erhalten kann. Verwenden Sie diese Option, um einen Teil der Netzwerkbandbreite für andere Aktivitäten im Netzwerk zu reservieren.

Voreinstellung ist: **Maximum.**

So stellen Sie die Netzwerkverbindungsgeschwindigkeit ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Datendurchsatz in Prozent bezogen auf die geschätzte maximale Netzwerkverbindungsgeschwindigkeit** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Datendurchsatz in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

4.7.5 Backup-Aufteilung

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist nicht wirksam, wenn das Backup-Ziel ein verwaltetes Depot oder der Acronis Cloud Storage ist.

Die Option definiert, wie ein Backup aufgeteilt werden kann.

Voreinstellung ist: **Automatisch**

Es stehen die folgenden Einstellungen zur Verfügung.

Automatisch

Mit dieser Einstellung wird Acronis Backup folgendermaßen arbeiten.

- **Bei Backups zu einem Festplattenlaufwerk oder eine Netzwerkfreigabe:**
  Es wird eine einzige Backup-Datei erstellt werden, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt.

Das Backup wird automatisch in mehrere Dateien aufgeteilt, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt. Das ist beispielsweise der Fall, wenn das Backup in einem FAT16- oder FAT32-Dateisystem mit einer Dateigrößenbeschränkung von 4 GB abgelegt wird.

Wenn das Ziellaufwerk während des Backups voll läuft, wechselt der Task in den Zustand **Benutzereingriff erforderlich**. Sie haben dann die Möglichkeit, zusätzlichen Speicherplatz frei zu machen und die Aktion zu wiederholen. In diesem Fall wird das resultierende Backup in zwei Teile gesplittet, die vor bzw. nach der Wiederholung erstellt wurden.

- **Beim Backup auf Wechselmedien** (CD, DVD, Blu-Ray Disc, einem autonomen Bandlaufwerk, einem RDX- oder USB-Laufwerk im Wechsellaufwerksmodus (S. 170)):

  Der Task wird in den Status **Benutzereingriff erforderlich** wechseln und nach einem neuen Medium fragen, wenn das vorhergehende voll ist.

- **Beim Backup auf einen FTP-Server:**

  Das Backup wird automatisch in Dateien von maximal 2 GB aufgeteilt. Die Aufteilung ist notwendig, damit eine Datenwiederherstellung direkt vom FTP-Server möglich ist.

- **Beim Backup auf einen SFTP-Server:**

  Eine einzelne Backup-Datei wird erstellt. Wenn der als Ziel verwendete Storage während des Backups voll läuft, schlägt der Task fehl.

Wenn Sie ein Backup replizieren oder verschieben (S. 79) (zu einem anderen Speicherort), dann gelten diese Regeln für jeden Speicherort unabhängig.

Beispiel:
Angenommen, dass der primäre Speicherort für ein 3-GB-Backup eine Festplatte ist, der zweite Speicherort ein FTP-Server und der dritte eine Netzwerkfreigabe. In diesem Fall wird das Backup in Form einer einzelnen Datei im primären Speicherort hinterlegt, in Form von zwei Dateien im zweiten Speicherort und wiederum als eine einzelne Datei im dritten Speicherort.

Feste Größe

Tragen Sie die gewünschte Dateigröße ein oder wählen Sie diese aus dem Listenfeld. Das Backup wird in mehrere Dateien der angegebenen Größe aufgeteilt. Das ist praktisch, wenn Sie ein Backup mit der Absicht erstellen, dieses nachträglich auf eine CD oder DVD zu brennen. Sie können ein Backup auch selbst in 2 GB große Dateien aufteilen, falls Sie die Sicherung zuerst auf ein Festplattenlaufwerk durchführen und planen, das Backup später manuell auf einen FTP-Server zu kopieren.

4.7.6 Komprimierungsrate

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Die Option definiert den Grad der Komprimierung für die zu sichernden Daten.

Voreinstellung ist: **Normal.**

Der ideale Grad für die Datenkomprimierung hängt von der Art der Daten ab, die gesichert werden sollen. So wird z.B. eine maximale Komprimierung die Größe einer Archivdatei nicht wesentlich beeinflussen, wenn bereits stark komprimierte Dateien im Archiv erfasst werden wie jpg-, pdf- oder mp3-Dateien. Andere Typen, wie z.B. doc- oder xls-Dateien, werden gut komprimiert.

So spezifizieren Sie den Komprimierungsgrad

Wählen Sie eine der nachfolgenden Varianten:

- **Keine** – die Daten werden so gesichert, wie sie sind, ohne dabei komprimiert zu werden. Die entstehende Größe des Backup-Archivs wird maximal sein.

- **Normal** – in den meisten Fällen empfohlen.
- **Hoch** – die Größe des entstehenden Backups ist üblicherweise kleiner als die bei der Einstellung **Normal**.
- **Maximum** – die Daten werden so sehr komprimiert, wie es geht. Die Dauer eines solchen Backups wird maximal sein. Sie könnten beim Backup auf Wechselmedien die maximale Komprimierung auswählen, um die Zahl der erforderlichen Medien zu verringern.

4.7.7 Desaster-Recovery-Plan (DRP)

Diese Option ist für Windows und Linux wirksam, aber nicht für Boot-Medium anwendbar.

Diese Option ist nicht für Datei-Backups wirksam.

Ein Desaster-Recovery-Plan (DRP) enthält eine Liste per Backup gesicherter Datenelemente sowie genaue Anweisungen, mit denen ein Benutzer durch den Prozess geführt wird, diese Elemente von einem Backup wiederherstellen zu können.

Ein DRP wird erstellt, sobald das erste Backup erfolgreich vom Backup-Plan durchgeführt wurde. Falls die Option **Desaster-Recovery-Pläne senden** aktiviert ist, wird der DRP per E-Mail an die spezifizierte Liste der Benutzer versendet. Falls die Option **DRP als Datei speichern** aktiviert ist, wird der DRP als Datei an dem spezifizierten Speicherort hinterlegt. Der DRP wird außerdem erneut in folgenden Fällen erstellt:

- Der Backup-Plan wurde bearbeitet, so dass sich die DRP-Parameter geändert haben.
- Das Backup enthält neue Datenelemente oder zuvor gesicherte Elemente sind nicht mehr enthalten. (Gilt nicht für Datenelemente wie Dateien oder Ordner.)

Sie können einen lokalen Ordner, einen Netzwerkordner, einen FTP- oder SFTP-Server als Ort zum Speichern der DRPs spezifizieren.

DRP und 'Nach'-Befehle für das Backup

Beachten Sie, dass der DRP nicht automatisch geändert wird, falls 'Nach'-Backup-Befehle Ihres Backup-Plans die Backups vom ursprünglichen Speicherort aus kopieren oder verschieben. Der DRP verweist nur auf die im Backup-Plan spezifizierten Speicherorte.

Einer DRP-Vorlage Informationen hinzufügen

Falls Sie mit XML und HTML vertraut sind, können Sie einer DRP-Vorlage (Template) zusätzliche Informationen hinzufügen. Die Standard-Pfade zur DRP-Vorlage sind:

- **%ProgramFiles%\Acronis\BackupAndRecovery\drp.xsl** – in einem 32 Bit Windows
- **%ProgramFiles(x86)%\Acronis\BackupAndRecovery\drp.xsl** – in einem 64 Bit Windows
- **/usr/lib/Acronis/BackupAndRecovery/drp.xsl** – in Linux

So konfigurieren Sie das Versenden von DRPs:

1. Aktivieren Sie das Kontrollkästchen **Desaster-Recovery-Pläne senden**.
2. Geben Sie die E-Mail-Adresse in das Eingabefeld **E-Mail-Adresse** ein. Sie können mehrere E-Mail-Adressen nacheinander eintragen, je durch Semikolon getrennt.
3. [Optional] Ändern Sie, falls erforderlich, das Feld **Betreff**.
4. Geben Sie die Parameter zum Zugriff auf den SMTP-Server ein. Zu weiteren Informationen siehe E-Mail-Benachrichtigungen (S. 144).
5. [Optional] Klicken Sie auf **Test-Mail senden**, um die Richtigkeit der Einstellungen zu überprüfen.

So konfigurieren Sie das Speichern der DRPs als Dateien:

1. Aktivieren Sie das Kontrollkästchen **DRP als Datei speichern**.
2. Klicken Sie auf **Durchsuchen**, um einen Speicherort für die DRP-Dateien zu spezifizieren.

4.7.8 E-Mail-Benachrichtigungen

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen über den erfolgreichen Abschluss von Backup-Tasks, über Fehler oder wenn ein Benutzereingriff erforderlich ist.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung senden**, um die entsprechende Funktion zu aktivieren.
2. Aktivieren Sie unter **E-Mail-Benachrichtigungen schicken** die entsprechenden Kontrollkästchen folgendermaßen:
   - **Wenn das Backup erfolgreich abgeschlossen wurde**.
   - **Wenn das Backup fehlschlägt**.
   - **Wenn Benutzereingriff erforderlich ist**.
3. Aktivieren Sie das Kontrollkästchen **Vollständiges Log zur Benachrichtigung hinzufügen**, falls Sie möchten, dass die E-Mail-Benachrichtigung Log-Einträge für die Aktion beinhalten soll.
4. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
5. Geben Sie im Feld **Betreff** eine Beschreibung für die Benachrichtigung ein.

   Die Betreffzeile kann gewöhnlichen Text und eine oder mehrere Variablen enthalten. In den empfangenen E-Mail-Nachrichten wird jede Variable dann durch den zum Zeitpunkt der Task-Ausführung vorliegenden Wert ersetzt. Folgende Variablen werden unterstützt:
   - **%description%**

     Bei einer unter Windows laufenden Maschine wird die Variable **%description%** durch einen Text ersetzt, der dem Feld **Computerbeschreibung** der jeweiligen Maschine entspricht. Um den Text spezifizieren zu können, können Sie entweder zu **Systemsteuerung –> System** gehen oder folgenden Befehl als Administrator ausführen:

     ```
     net config server /srvcomment:<text>
     ```

     Bei einer unter Linux laufenden Maschine wird die Variable **%description%** durch einen leeren String ("") ersetzt.
   - **%subject%**

     Die Variable **%subject%** wird in folgenden Ausdruck umgewandelt: *Task <Task-Name> <Task-Ergebnis> auf Maschine <Maschinenname>.*
6. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
7. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
8. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.

9. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:
   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.
   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
      - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
      - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
      - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.
   d. Klicken Sie auf **OK**.
10. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

4.7.9 Fehlerbehandlung

Diese Optionen sind für Windows- und Linux-Betriebssysteme sowie Boot-Medien wirksam.

Mit diesen Optionen können Sie festlegen, wie eventuell auftretende Fehler beim Backup behandelt werden.

Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)

Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die eine Benutzeraktion erfordern (außer der Behandlung von fehlerhaften Sektoren, die mit einer eigenen Option gesteuert wird). Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler erneut versuchen

Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Abstand zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Wenn der Speicherort des Backups im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

*Sollte der Acronis Cloud Storage als erster, zweiter oder ein weiterer Backup-Speicherort ausgewählt sein, dann lautet die automatische Einstellung des Optionswerts **Aktiviert. Anzahl der Versuche: 300**, unabhängig vom Standardwert.*

Fehlerhafte Sektoren ignorieren

Voreinstellung ist: **Deaktiviert**.

Wenn die Option unwirksam gemacht ist, wird das Programm jedes Mal ein Pop-up-Fenster zeigen, wenn es auf einen fehlerhaften Sektor stößt, und um eine Entscheidung bitten, ob das Backup fortgesetzt oder abgebrochen werden soll. Wenn Sie z.B. vorhaben, die Informationen von einer 'sterbenden' Festplatte zu retten, aktivieren Sie diese Funktion. Die restlichen Daten werden in diesem Fall noch gesichert und Sie werden das entstandene Laufwerk-Backup mounten und die noch gültigen Daten auf ein anderes Laufwerk kopieren können.

4.7.10 Ereignisverfolgung

Es ist möglich, die von den Backup-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

4.7.10.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Backup-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup siehe „Unterstützung für SNMP (S. 34)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

So wählen Sie, ob Ereignisse von Backup-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **SNMP-Benachrichtigungen für Ereignisse bei Backup-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Backup-Aktionen an spezifizierte SNMP-Manager.
  - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
  - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
  - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

- **Keine SNMP-Benachrichtigungen senden** – Einstellung, um das Versenden von Ereignissen über Backup-Aktionen an SNMP-Manager unwirksam zu machen.

4.7.10.2 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Backup-Aktionen in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

Wählen Sie, ob Ereigniseinträge der Backup-Aktionen an die Ereignisanzeige von Windows übergeben werden.

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Backup-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
  - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
  - **Fehler und Warnungen**
  - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Backup-Aktionen in der Ereignisanzeige.

4.7.11 Beschleunigtes inkrementelles und differentielles Backup

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für inkrementelle und differentielle Backups auf Dateiebene.

Diese Option definiert, ob für die Ermittlung einer Dateiänderung die Dateigröße und der Zeitstempel benutzt werden oder dafür der Dateiinhalt mit den im Archiv gespeicherten Dateien verglichen wird.

Voreinstellung ist: **Aktiviert.**

Inkrementelle oder differentielle Backups erfassen nur die geänderten Daten. Um das Backup-Verfahren zu beschleunigen, entscheidet das Programm darüber, ob eine Datei geändert wurde oder nicht, anhand von Dateigröße und Zeitstempel der letzten Änderung. Das Ausschalten dieser Funktion wird dazu führen, dass das Programm immer den Inhalt einer Datei mit dem Inhalt der Datei vergleicht, die in einem Archiv gespeichert ist.

4.7.12 Snapshot für Backup auf Dateiebene

Diese Option ist nur für Backups auf Dateiebene wirksam in Windows- und Linux-Betriebssystemen.

Diese Option definiert, ob Dateien eine nach der anderen gesichert werden oder auf Basis eines sofortigen Snapshots der Daten.

Beachten Sie: *Dateien von Netzlaufwerken werden immer eine nach der anderen gesichert.*

Voreinstellung ist: **Snapshot erstellen, wenn es möglich ist.**

Wählen Sie eine der nachfolgenden Varianten:

- **Immer einen Snapshot erstellen**

  Ein Snapshot ermöglicht das Backup aller Dateien einschließlich solcher, die für den exklusiven Zugriff geöffnet sind. Die Dateien werden zum gleichen Zeitpunkt gesichert. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Um einen Snapshot zu benutzen, muss der Backup-Plan mit einem Administrator-Konto oder den Rechten eines Backup-Operators ausgeführt werden. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.

- **Snapshot erstellen, wenn es möglich ist**

  Dateien direkt sichern, wenn kein Snapshot möglich ist.

- **Keinen Snapshot erstellen**

  Dateien immer direkt sichern. Administratorrechte oder Rechte eines Backup-Operators sind nicht erforderlich. Der Versuch zum Sichern von Dateien, die für exklusiven Zugriff geöffnet sind, wird in einem Fehler resultieren. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

4.7.13 Sicherheit auf Dateiebene

Diese Optionen sind nur für Backups auf Dateiebene unter Windows-Betriebssystemen wirksam.

Verschlüsselte Dateien in Archiven unverschlüsselt speichern

Diese Option definiert, ob die Dateien vor der Speicherung im Archiv entschlüsselt werden.

Voreinstellung ist: **Ausgeschaltet**.

Ignorieren Sie diese Option, wenn Sie keine Verschlüsselung benutzen. Aktivieren Sie diese Option, wenn verschlüsselte Dateien in das Backup einbezogen werden und Sie wollen, dass ein beliebiger Benutzer nach der Wiederherstellung auf die Dateien zugreifen kann. Andernfalls wird nur der Benutzer, der die Dateien bzw. Verzeichnisse ursprünglich verschlüsselt hat, darauf zugreifen können. Die Entschlüsselung ist auch nützlich, wenn Sie verschlüsselte Dateien auf verschiedenen Maschinen wiederherstellen wollen.

Die Dateiverschlüsselung steht in Windows zur Verfügung unter Verwendung des NTFS-Dateisystems mit Encrypting File System (EFS). Um auf die Verschlüsselungseinstellungen einer Datei oder eines Verzeichnisses zugreifen, wählen Sie ***Eigenschaften > Allgemein > Erweitert> Inhalt verschlüsseln****.*

Dateisicherheitseinstellungen in Archiven erhalten

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien gesichert werden.

Voreinstellung ist: **Aktiviert.**

Wenn die Option eingeschaltet ist, werden Dateien und Ordner mit der ursprünglichen Erlaubnis zum Lesen, Schreiben oder Ausführen für jeden Benutzer oder jede Benutzergruppe im Archiv gespeichert. Wenn Sie auf einer Maschine geschützte Dateien bzw. Ordner ohne den in den Berechtigungen angegebenen Benutzer wiederherstellen, werden Sie wahrscheinlich nicht in der Lage sein, diese Dateien bzw. Ordner zu lesen oder zu verändern.

Um dieses Problem zu beseitigen, sollten Sie die Aufbewahrung von Dateisicherheitseinstellungen in Archiven unwirksam machen. Die wiederhergestellten Dateien und Ordner erben dann immer die Rechte des Ordners, in den sie wiederhergestellt werden, oder die der Festplatte, wenn sie an der Wurzel wiederhergestellt werden.

Alternativ können Sie die Wiederherstellung (S. 147) der Sicherheitseinstellungen unwirksam machen, selbst wenn diese im Archiv gespeichert sind. Das Ergebnis wird das gleiche sein – die Dateien erben die Zugriffsrechte vom übergeordneten Ordner.

*Um auf die NTFS-Zugriffsrechte von Datei oder Ordnern zuzugreifen, wählen Sie **Eigenschaften** > **Sicherheit**>.*

4.7.14 Medienkomponenten

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam, wenn das Ziel des Backups CDs, DVDs oder Blue-ray Discs (BD) sind.

Wenn Sie ein Backup auf ein solches Medium speichern, dann können Sie dieses Medium zu einem Linux-basierten bootfähigen Medium (S. 296) machen, indem Sie zusätzliche Komponenten darauf speichern. Als Konsequenz benötigen Sie kein separates Notfallmedium.

Voreinstellung ist: **Keine bootfähigen Komponenten.**

Wählen Sie eine der folgenden Komponenten, die Sie auf das bootfähige Medium platzieren wollen:

- Der **Acronis Bootable Agent** ist ein bootfähiges, auf einem Linux-Kernel basierendes Notfallwerkzeug, das die meisten Funktionen des Acronis Backup Agenten enthält. Platzieren Sie diese Komponente auf dem Medium, wenn Sie größere Funktionalität während der Wiederherstellung wünschen. Sie können die Wiederherstellung auf die gleiche Weise wie von einem regulären Boot-Medium konfigurieren und Active Restore oder Universal Restore verwenden. Wenn das Medium in Windows erstellt wird, stehen auch die Funktionen zur Laufwerksverwaltung zur Verfügung.
- **Acronis Bootable Agent und One-Click Restore**. One-Click Restore ist eine kleine Ergänzung zu einem Laufwerk-Backup, das auf einem Wechselmedium gespeichert ist, welche auf einen einzelnen Klick hin eine Wiederherstellung dieses Backups ermöglicht. Wenn Sie eine Maschine von diesem Medium starten und auf **Acronis One-Click Restore ausführen** klicken, dann wird das Laufwerk unmittelbar aus dem Backup wiederhergestellt, das auf dem gleichen Medium enthalten ist.

  ***Achtung:** Weil diese Art der Wiederherstellung keine Interaktionaktionsmöglichkeit für den Benutzers bietet, wie z.B. die Auswahl der wiederherzustellenden Volumes, stellt Acronis One-Click Restore immer das komplette Laufwerk wieder her. Falls das Laufwerk also mehrere Volumes enthält und Sie den Einsatz von Acronis One-Click Restore planen, dann müssen Sie alle Volumes in das Backup aufnehmen. Ansonsten gehen beim Einsatz dieser Funktion die Volumes verloren, die nicht im Backup enthalten sind.*

4.7.15 Mount-Punkte

Diese Option ist nur unter Windows und für ein Datei-basiertes Backup wirksam, dessen Datenquelle gemountete Volumes oder freigegebene Cluster-Volumes enthält.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. (Ein Mount-Punkt ist ein Ordner, an den ein zusätzliches Volume logisch angebunden ist).

- Wenn ein solcher Ordner (oder ein übergeordneter Ordner) als Backup-Quelle ausgewählt wird – und die Option **Mount-Punkte** aktiviert wurde – dann werden alle auf dem gemounteten Volume

liegenden Dateien in das Backup aufgenommen. Wenn die Option **Mount-Punkte** deaktiviert wurde, bleibt der Mount-Punkt im Backup leer.

Bei der Wiederherstellung eines übergeordneten Ordners hängt die Frage, ob auch der Inhalt des Mount-Punktes wiederhergestellt wird (oder nicht) davon ab, ob die Option **Mount-Punkte** für die Recovery-Aktion (S. 147) aktiviert oder deaktiviert wurde.

- Wenn Sie den Mount-Punkt direkt auswählen oder einen Ordner innerhalb des gemounteten Volumes, dann werden die gewählten Ordner wie herkömmliche Ordner betrachtet. Sie werden unabhängig vom Status der Backup-Option **Mount-Punkte** gesichert – genauso, wie sie unabhängig vom Status der entsprechenden Recovery-Option **Mount-Punkte**für die Recovery-Aktion (S. 147) wiederhergestellt werden.

Voreinstellung ist: **Deaktiviert**.

Tipp: *Sie können virtuelle Maschinen vom Typ Hyper-V sichern, die auf einem freigegebenen Cluster-Volume liegen, indem Sie die benötigten Dateien oder das komplette Volume per Datei-basiertem Backup sichern. Fahren Sie die virtuellen Maschinen herunter, um zu gewährleisten, dass sie in einem konsistenten Zustand gesichert werden.*

Beispiel

Angenommen, der Ordner **C:\Daten1** ist der Mount-Punkt für ein gemountetes Volume. Das Volume enthält die Verzeichnisse **Ordner1** und **Ordner2**. Sie erstellen einen Backup-Plan zur Datei-basierten Sicherung Ihrer Daten.

Wenn Sie das Volume C per Kontrollkästchen auswählen und dafür die Option **Mount-Punkte** aktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup auch die Verzeichnisse **Ordner1** und **Ordner2** enthalten. Wenn Sie die gesicherten Daten dann später wiederherstellen, sollten Sie an die entsprechende, gewünschte Einstellung der Option **Mount-Punkte** für die Recovery-Aktionen (S. 147) denken.

Wenn Sie das Volume C per Kontrollkästchen auswählen und die Option **Mount-Punkte** jedoch deaktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup leer sein.

Wenn Sie die Verzeichnisse **Daten1**, **Ordner1** oder **Ordner2** direkt selbst per Kontrollkästchen zum Backup auswählen, werden diese markierten Ordner wie herkömmliche Ordners in Backup aufgenommen – unabhängig vom Status der Option **Mount-Punkte**.

4.7.16 Multi-Volume-Snapshot

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Diese Option gilt für Backups auf Laufwerksebene. Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot für Backup auf Dateiebene (S. 99) bestimmt, ob bei einem solchen Backup ein Snapshot benutzt wird oder nicht.)

Die Option bestimmt, ob Snapshots mehrerer Volumes gleichzeitig oder einer nach dem anderen erfasst werden sollen.

Voreinstellung ist: **Aktivieren.**

Wenn diese Option auf **Aktivieren** gesetzt wird, werden die Snapshots aller zu sichernden Volumes zum gleichen Zeitpunkt erstellt. Benutzen Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Volumes verteilt sind, z.B. für eine Oracle-Datenbank.

Wenn diese Option auf **Deaktivieren** gesetzt wird, erfolgen die Snapshots der Volumes nacheinander. Falls sich also Daten über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert und das resultierende Backup könnte nicht konsistent sein.

4.7.17 Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach einem Backup durchgeführt werden.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

Befehl vor dem Backup	Backup	Befehl nach Backup

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Löschen Sie bestimmte temporäre Dateien von der Festplatte, bevor ein Backup gestartet wird.
- Konfiguration Sie das Antivirenprodukt eines Drittanbieters so, dass es vor jedem Start des Backups ausgeführt wird.
- Kopieren Sie Backups selektiv von einem Archiv zu einem anderen Speicherort. Diese Option kann nützlich sein, weil die in einem Backup-Plan konfigurierte Replikation *jedes* Backup eines Archivs zu den nachfolgenden Speicherorten kopiert.

Acronis Backup führt die Replikation *nach* Ausführung des Nach-Backup-Befehls aus. Weitere Informationen finden Sie unter 'Die Reihenfolge von Aktionen in einem Backup-Plan (S. 60)'.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. „pause“.

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Backup ausführen**
   - **Nach Backup ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

4.7.17.1 Befehl vor Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start des Backups ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.

4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Kein Backup, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Backup nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.17.2 Befehl nach Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn das Backup vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** ein Kommando ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
3. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
4. Aktivieren Sie das Kontrollkästchen **Task scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Falls die Befehlsausführung versagt, wird das Programm die entstehende tib-Datei sowie temporäre Dateien sofern möglich entfernen – das Task-Ergebnis wird zudem auf 'Fehlgeschlagen' gesetzt.

   Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Einsicht in das Log verfolgen – oder über die Fehler- bzw. Warnmeldungen, die in der Ansicht **Log** angezeigt werden.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

4.7.18 Befehle vor/nach der Datenerfassung

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenerfassung (also Erstellung des Daten-Snapshots) durchgeführt werden. Die Datenerfassung wird von Acronis Backup zu Beginn der Backup-Prozedur durchgeführt.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

	<--------------- **Backup** --------------->				
Befehl vor Backup	Befehl vor Datenerfassung	Datener-fassung	Befehl nach Datenerfassung		Befehl nach Backup

Wenn die Option Volume Shadow Copy Service (S. 109) aktiviert ist, werden die Ausführung der Befehle und die Aktionen von Microsofts VSS folgendermaßen eingeordnet:

Befehle „vor Datenerfassung“ -> VSS Suspend -> Datenerfassung -> VSS Resume -> Befehle „nach Datenerfassung“.

Mit Hilfe der Befehle vor bzw. nach der Datenerfassung können Sie Datenbanken, die nicht mit VSS kompatibel sind, vor der Datenerfassung suspendieren und nach der Datenerfassung wieder anlaufen lassen. Im Gegensatz zu den Vor-/Nach-Befehlen (S. 103) werden die Befehle vor/nach der Datenerfassung direkt vor bzw. nach dem Datenerfassungsprozess durchgeführt. Das benötigt einige Sekunden. Die komplette Backup-Prozedur kann in Abhängigkeit von der zu sichernden Datenmenge entsprechend deutlich länger dauern. Daher werden die Datenbanken oder die Anwendungen nur kurze Zeit pausieren.

So spezifizieren Sie Befehle vor/nach der Datenerfassung

1. Sie aktivieren Befehle vor/nach der Datenerfassung mit Hilfe der folgenden Optionen:
   - **Vor der Datenerfassung ausführen**
   - **Nach der Datenerfassung ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

4.7.18.1 Befehl vor Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	Auswahl			
Backup-Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Keine Datenerfassung, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Datenerfassung nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Datenerfassung gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.18.2 Befehl nach Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die nach der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	Auswahl			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Kein Backup, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert

Ergebnis				
	Voreinstellung Backup nur fortsetzen, nachdem der Befehl erfolgreich durchgeführt wurde. Löschen der tib-Datei und temporären Dateien sowie Task fehlschlagen lassen, wenn die Befehlsausführung versagt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung fortsetzen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.19 Inaktivitätszeit für Replikation/Bereinigung

Diese Option ist nur wirksam, wenn Sie für Backups entweder Replikation oder Aufbewahrungsregeln (S. 79) einrichten.

Die Option definiert einen Zeitraum, in dem der Start einer Replikation oder die Anwendung von Aufbewahrungsregeln nicht erlaubt ist. Diese Aktionen werden daher dann ausgeführt, wenn die Inaktivitätszeit beendet ist und sofern die Maschine zu diesem Zeitpunkt eingeschaltet ist. Aktionen, die vor dem Inaktivitätszeitraum gestartet wurden, werden ohne Unterbrechung fortgesetzt.

Die Inaktivitätszeit betrifft alle Speicherorte, den primären eingeschlossen.

Voreinstellung ist: **Deaktiviert.**

Aktivieren Sie zur Spezifikation der Inaktivitätszeit das Kontrollkästchen **Replikation/Bereinigung in folgender Zeit nicht starten** und wählen Sie dann die Tage und den entsprechenden Zeitraum.

Anwendungsbeispiele

Sie können diese Option auf Wunsch verwenden, um den eigentlichen Backup-Prozess von der Replikation oder Bereinigung zu separieren. Nehmen Sie beispielsweise an, dass Sie Maschinen lokal sowie tagsüber sichern und die entsprechenden Backups dann zu einem Netzwerkordner replizieren. Stellen Sie die Inaktivitätszeit so ein, dass sie die reguläre Arbeitszeit enthält. Die Replikation wird daraufhin nach diesen Arbeitstunden gemacht, wenn auch die Netzwerklast geringer ist.

4.7.20 Sektor-für-Sektor-Backup

Die Option ist nur für Backups auf Laufwerksebene wirksam.

Aktivieren Sie das Kontrollkästchen **Sektor-für-Sektor sichern**, um von einem Laufwerk bzw. Volume auf physikalischer Ebene eine exakte Kopie zu erstellen. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option **Komprimierungsgrad** (S. 94) auf **Keine** eingestellt ist). Verwenden Sie das Sektor-für-Sektor-Backup, um Laufwerke mit nicht erkanntem oder nicht unterstütztem Dateisystem und anderen proprietären Datenformaten zu sichern.

4.7.21 Task-Fehlerbehandlung

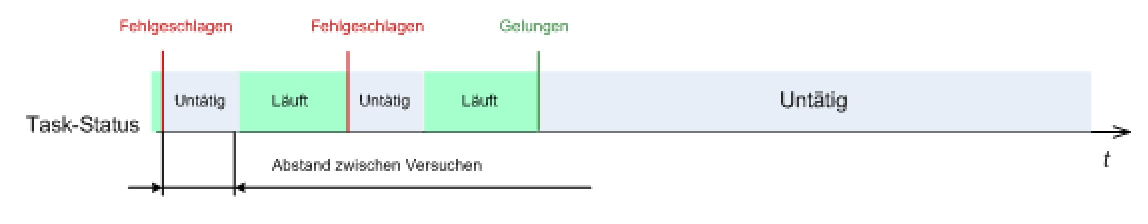
Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

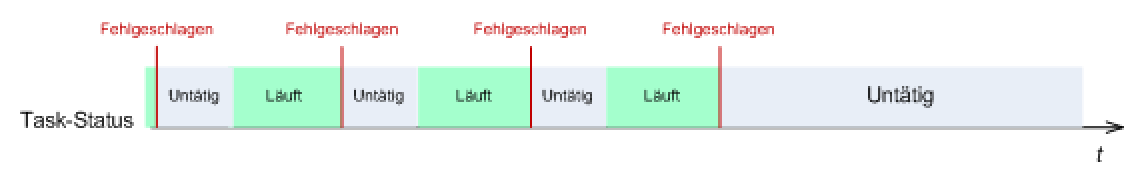
Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, wenn irgendein Task eines Backup-Plans versagt.

Die Voreinstellung ist **Fehlgeschlagenen Task nicht erneut starten.**

Wenn Sie das Kontrollkästchen **Fehlgeschlagenen Task erneut starten** aktivieren und die Anzahl der Versuche sowie den Zeitabstand zwischen den Versuchen angeben, versucht das Programm, den fehlgeschlagenen Task erneut zu starten. Die Versuche werden aufgegeben, wenn entweder die Aktion gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.





Wenn ein Task aufgrund eines Fehlers im Backup-Plan fehlgeschlagen ist, können Sie den Plan bearbeiten, während der Task untätig ist. Während der Task dagegen läuft, müssen Sie ihn stoppen, bevor Sie den Backup-Plan bearbeiten können.

4.7.22 Task-Startbedingungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, falls ein Backup-Task starten will (die eingestellte Zeit ist gekommen oder das spezifizierte Ereignis ist eingetreten), aber die Bedingung (oder eine der Bedingungen) nicht erfüllt ist. Weitere Informationen über Bedingungen finden Sie unter Planen (S. 66) und Bedingungen (S. 76).

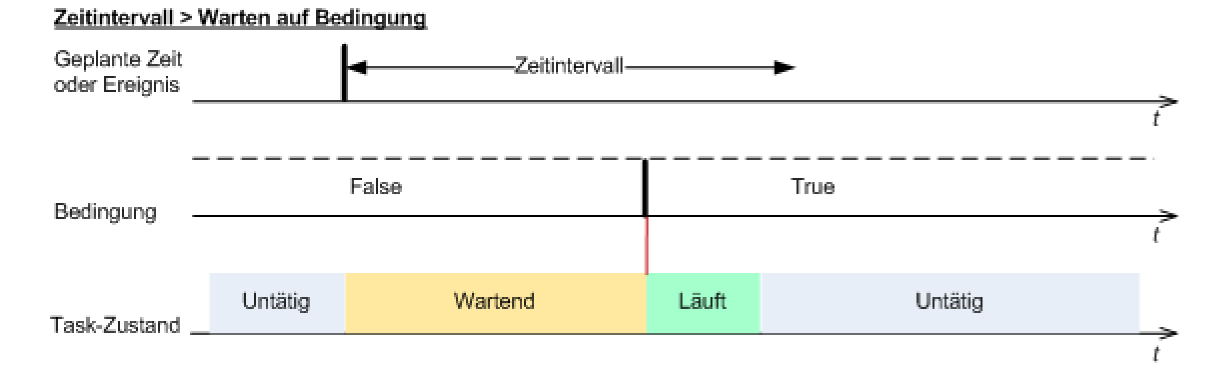
Voreinstellung ist: **Warten, bis die Bedingungen erfüllt sind.**

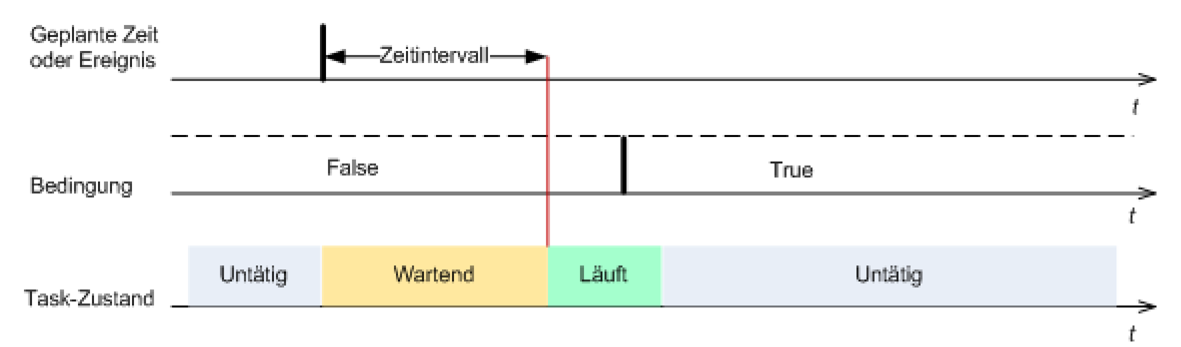
Warten, bis die Bedingungen erfüllt sind

Mit dieser Einstellung beginnt der Scheduler mit dem Überwachen der Bedingungen und schließt die Aufgabe ab, sobald die Bedingungen erfüllt sind. Wenn die Bedingungen nie erfüllt sind, wird der Task nie starten.

Um zu reagieren, wenn die Bedingungen für zu lange Zeit nicht erfüllt wurden und ein weiteres Verschieben des Backups zu riskant erscheint, können Sie einen Zeitabstand einstellen, nach dessen Ablauf der Task unabhängig von der Erfüllung der Bedingungen starten wird. Aktivieren Sie das Kontrollkästchen **Task trotzdem ausführen nach** und geben Sie dann den Zeitabstand an. Der Task wird starten, sobald die Bedingungen erfüllt sind ODER die Zeitspanne abgelaufen ist, je nachdem, was als Erstes eintritt.

Zeit-Diagramm: Warten, bis die Bedingungen erfüllt sind





Ausführung des Tasks übergehen

Das Verschieben eines Backups könnte nicht akzeptabel sein, wenn Sie z.B. ein Backup unbedingt zu einer angegebenen Zeit ausführen müssen. Dann macht es eher Sinn, das Backup zu übergehen, anstatt auf die Erfüllung der Bedingungen zu warten, besonders wenn die Ereignisse verhältnismäßig oft stattfinden.

4.7.23 Volume Shadow Copy Service

Diese Optionen sind nur für Windows-Betriebssysteme wirksam.

Den Volume Shadow Copy Service verwenden

Diese Option definiert, ob ein VSS-Provider (Volume Shadow Copy Service) VSS-kompatible Anwendungen benachrichtigen muss, dass ein Backup startet. Dies sichert einen konsistenten Zustand aller Daten, die von Anwendungen benutzt werden, vor allem aber die Vollendung aller Datenbanktransaktionen für den Moment, in dem Acronis Backup den Snapshot erstellt. Die Datenkonsistenz wiederum gewährleistet vor allem, dass Anwendungen in einem korrekten Zustand wiederhergestellt werden und unmittelbar nach der Wiederherstellung einsatzbereit sind.

Voreinstellung ist: **Volume Shadow Copy Service verwenden**.

VSS verwenden

Wenn die Option **Volume Shadow Copy Service verwenden** aktiviert ist, dann wählen Sie einen Snapshot-Provider aus folgender Liste:

- **Hardware/Software – Automatisch wählen**

  VSS wird denjenigen Hardware-basierten Provider verwenden, der das Quell-Volume unterstützt. Wird keiner gefunden, dann verwendet der VSS den Acronis VSS Provider.

- **Software – Automatisch wählen**

  In den meisten Fällen wird der VSS den Acronis VSS Provider verwenden.
- **Software – Acronis VSS Provider**

  VSS wird den Acronis VSS Provider zum Erstellen von Snapshots verwenden.
- **Software – System-Provider** (standardmäßig voreingestellt)

  VSS wird den Provider des Systems (Microsoft Software Shadow Copy Provider) zum Erstellen von Snapshots verwenden. Wir empfehlen, beim Backup von Anwendungsservern (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint oder Active Directory) den System-Provider zu verwenden.
- **Software – Ein Software-Provider**

  In den meisten Fällen wird der VSS den Microsoft Software Shadow Copy Provider verwenden.
- **Hardware – Automatisch wählen**

  VSS wird denjenigen Hardware-basierten Provider verwenden, der das Quell-Volume unterstützt. Wird kein Hardware-basierter Provider gefunden, dann werden die Backups von Acronis Backup ohne die Erfassung von Snapshots erstellt.

Hinweis: *Die Verwendung eines Hardware Snapshot Providers erfordert möglicherweise administrative Berechtigungen.*

VSS nicht verwenden

Wenn Sie die Option **VSS nicht verwenden** aktivieren, werden die Daten-Snapshots durch Acronis Backup erstellt.

Verwenden Sie die Option **VSS nicht verwenden**, wenn Ihre Datenbank mit VSS nicht kompatibel ist. Der Backup-Prozess ist am schnellsten, aber die Datenkonsistenz von Anwendungen, deren Transaktionen zum Zeitpunkt des Snapshots nicht vollendet sind, kann nicht garantiert werden. Sie können Befehle vor/nach der Datenerfassung (S. 104) verwenden, um festzulegen, welche Befehle vor und nach Erfassung des Snapshots ausgeführt werden sollen. Das gewährleistet, dass die Daten in einem konsistenten Zustand gesichert werden. Spezifizieren Sie z.B. einen Befehl vor der Datenerfassung, der diese Datenbank anhält und alle Cache-Speicher leert, um zu sichern, dass alle Transaktionen vollendet sind – und ergänzen Sie Befehle nach der Datenerfassung, damit die Datenbank nach der Snapshot-Erstellung den Betrieb wieder aufnimmt.

Über Volume Shadow Copy Writer

Bevor Sie die Daten einer VSS-kompatiblen Anwendung sichern, überprüfen Sie, dass die Volume Shadow Copy Writer für diese Anwendung eingeschaltet sind – und zwar, indem Sie die Liste der Writer untersuchen, die im Betriebssystem präsent sind. Verwenden Sie folgenden Befehl, um diese Liste einzusehen:

```
vssadmin list writers
```

Hinweis: *In Microsoft Windows Small Business Server 2003 ist der Writer für Microsoft Exchange Server 2003 als Standardvorgabe ausgeschaltet. Informationen zum Anschalten des Schreibers finden Sie im Microsoft Knowledge Base-Artikel http://support.microsoft.com/kb/838183/ .*

VSS-Voll-Backup aktivieren

Voreinstellung ist: **Deaktiviert**.

Diese Option kann nützlich sein, wenn Sie Microsoft Exchange-Server mit einem Laufwerk-Backup schützen (S. 222).

Sofern aktiviert, werden die Protokolle des Microsoft Exchange Servers und anderer VSS-kompatibler Anwendungen (mit Ausnahme des Microsoft SQL Servers) nach jedem erfolgreichen vollständigen, inkrementellen oder differentiellen Backup abgeschnitten.

Lassen Sie diese Option in folgenden Fällen deaktiviert:

- Falls Sie den Acronis Backup Agenten für Exchange oder eine Dritthersteller-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Dritthersteller-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Dritthersteller-Software das resultierende Laufwerk-Backup als sein eigenes Voll-Backup ansehen wird. Als Folge wird das nächste differentielle Backup der SQL Server-Daten fehlschlagen. Die Backups werden solange fehlschlagen, bis die Dritthersteller-Software das nächste eigene Voll-Backup erstellt.
- Falls andere VSS-kompatible Anwendungen auf der Maschine laufen und es aus irgendwelchen Gründen notwendig ist, deren Protokolle zu behalten.

Eine Aktivierung dieser Option bewirkt kein Abschneiden von Microsoft SQL Server-Protokollen. Um das SQL Server-Protokoll nach einem Single-Pass-Backup (Einzeldurchlauf-Backup) abzuschneiden, müssen Sie die Einstellung **Protokollabschneidung** im Bereich **Single-Pass-Laufwerk- und Anwendungs-Backup** der Seite **Backup-Plan erstellen** oder **Backup jetzt** aktivieren.

Aktivieren Sie diese Option, wenn Sie VSS (virtueller Schattenkopie-Dienst) auf einer Maschine verwenden, die Windows XP verwendet und den Microsoft SQL Server ausführt. Falls Sie die Option deaktiviert lassen, kann das Backup fehlschlagen.

5 Recovery

Wenn eine Datenwiederherstellung ansteht, sollten Sie als Erstes erwägen, welches die funktionellste Methode ist: Verbinden Sie die Konsole mit der verwalteten, **das Betriebssystem ausführenden Maschine** und erstellen Sie den Recovery-Task.

Sollte auf der Maschine **das Betriebssystem nicht mehr starten** oder sollten Sie eine **Wiederherstellung auf fabrikneuer Hardware** durchführen müssen, dann booten Sie die Maschine mit einem bootfähigen Medium (S. 296) oder dem Acronis Startup Recovery Manager und konfigurieren Sie dann die Wiederherstellung.

Acronis Universal Restore ermöglicht Ihnen, Betriebssysteme **auf abweichender Hardware** oder einer virtuellen Maschine wiederherzustellen und von diesen zu booten.

Acronis Backup ermöglicht Ihnen, Windows-Betriebssystemen zwischen BIOS-basierter Hardware und UEFI-unterstütztender Hardware (Unified Extensible Firmware Interface) zu übertragen. Zu weiteren Details siehe den Abschnitt 'BIOS-basierte Systeme zu UEFI-basierten wiederherstellen und umgekehrt (S. 131)'.

Ein **Windows-System kann in Sekunden wieder online gebracht werden**, noch während die Wiederherstellung im Hintergrund abläuft. Dank der proprietären Technologie Acronis Active Restore (S. 135) kann Acronis Backup die Maschine in das im Backup vorliegende Betriebssystem 'hinein' booten – ganz so, als ob das System auf einer physikalischen Laufwerk vorliegen würde. Das System wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Auf diese Weise bleibt die Ausfallszeit des Systems minimal.

Ein dynamisches Volume kann über ein bereits existierendes Volume, den 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe oder den 'nicht zugeordneten' Speicherplatz eines einzelnen Basis-Laufwerks wiederhergestellt werden. Um mehr über die Wiederherstellung dynamischer Volumes zu erfahren, wechseln Sie zum Abschnitt 'Backup und Recovery von dynamischen Volumes (Windows) (S. 30)'.

Der Acronis Backup Agent für Windows hat die Fähigkeit, ein Laufwerk- bzw. Volume-Backup zu einer neuen virtuellen Maschine wiederherzustellen. Weitere Informationen finden Sie im Abschnitt 'Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 157).

Sie müssen möglicherweise vor einer Wiederherstellung die Ziellaufwerke vorbereiten. Acronis Backup enthält ein nützliches Werkzeug zur Laufwerksverwaltung, welches Ihnen erlaubt, Volumes zu erstellen oder zu löschen, das Partitionsschema eines Laufwerks zu ändern, eine Laufwerksgruppe zu erstellen und andere Laufwerksverwaltungsaktionen auf der Ziel-Hardware durchzuführen (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director LV siehe den Abschnitt 'Laufwerksverwaltung (S. 204)'.

5.1 Einen Recovery-Task erstellen

Zur Erstellung eines Recovery-Tasks führen Sie folgende Schritte aus

Recovery-Quelle

Daten wählen (S. 114)

Wählen Sie die wiederherzustellenden Daten.

Anmeldedaten (S. 118)

[Optional] Stellen Sie Anmeldedaten für den Speicherort des Archivs zur Verfügung, falls das Benutzerkonto des Tasks für diesen keine Zugriffserlaubnis hat. Klicken Sie auf **Anmeldedaten anzeigen**, um auf diese Option zugreifen zu können.

Recovery-Ziel

Dieser Abschnitt erscheint, nachdem das benötigte Backup gewählt und der wiederherzustellende Datentyp definiert wurde. Die von Ihnen hier anzugebenden Parameter hängen vom wiederherzustellenden Datentyp ab.

Laufwerke (S. 119)

Volumes (S. 122)

Dateien (S. 126)

Acronis Active Restore (S. 135)

Gilt für: Recovery von Systemlaufwerken oder Volumes.

[Optional] Aktivieren Sie bei Bedarf Acronis Active Restore, falls Sie ein System direkt nach dem Start der Wiederherstellung einsatzbereit haben (online bringen) müssen.

Anmeldedaten (S. 118)

[Optional] Stellen Sie die Anmeldedaten für den Zielort zur Verfügung, falls mit den Anmeldedaten des Tasks keine Wiederherstellung der Daten möglich ist. Klicken Sie auf **Anmeldedaten anzeigen**, um auf diese Einstellung zugreifen zu können.

Recovery-Zeitpunkt

Recovery (S. 127)

Bestimmen Sie, wann die Wiederherstellung beginnen soll. Der Task kann unmittelbar nach Erstellung starten, für einen bestimmten Tag bzw. Zeitpunkt geplant werden oder auch einfach nur zur manuellen Ausführung gespeichert werden.

Task-Parameter

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Recovery-Task ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Recovery-Optionen

[Optional] Passen Sie die Aktion durch Konfiguration der Recovery-Optionen an, z.B. Vor-/Nach-Befehle, Recovery-Priorität, Fehlerhandhabung oder Benachrichtigungsoptionen. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 141) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert in einer neuen Zeile angezeigt. Die Statusanzeige über die Einstellungen ändert sich von **Standard** zu **Benutzerdefiniert**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Wenn der Standardwert eingestellt wird, verschwindet die Zeile. Sie sehen daher in diesem Abschnitt immer nur die Einstellungen, die von den Standardwerten abweichen.

Ein Klick auf **Auf Standard zurücksetzen** setzt alle Einstellungen auf die Standardwerte zurück.

Anmeldedaten für den Task

[Optional] Der Task wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Konto-Anmeldedaten für den Task ändern. Klicken Sie auf **Anmeldedaten des Tasks anzeigen**, um auf diese Einstellung zugreifen zu können.

[Optional] Universal Restore

Gilt für: Recovery von Systemlaufwerken oder Volumes.

Universal Restore (S. 128)

Verwenden Sie Acronis Universal Restore, wenn Sie ein Betriebssystem auf abweichender Hardware wiederherstellen und booten müssen.

Klicken Sie nach Abschluss aller notwendiger Schritte auf **OK**, um den Recovery-Task zu erstellen.

5.1.1 Recovery-Quelle

1. Spezifizieren Sie den Archiv-Speicherort

Spezifizieren Sie im Feld **Datenpfad** den Pfad zum Archiv-Speicherort oder klicken Sie auf **Durchsuchen** und wählen Sie den gewünschten Speicherort (wie im Abschnitt 'Speicherort für Archive wählen (S. 115)' beschrieben) aus.

2. Daten wählen

Sie können die gesicherten Daten entweder über die Registerlasche **Datenanzeige** oder **Archiv-Anzeige** auswählen. In der Registerlasche **Datenanzeige** werden alle gesicherten Daten innerhalb des gewählten Archiv-Speicherortes nach Versionen angezeigt (also dem Zeitpunkt der Backup-Erstellung). In der Registerlasche **Archiv-Anzeige** werden die gesicherten Daten nach Archiven angezeigt.

Daten in der Datenanzeige auswählen

Da die Registerlasche **Datenanzeige** seine Funktionalität mit dem Datenkatalog teilt, erfolgt die Datenauswahl in der Registerlasche **Datenanzeige** genauso wie im Datenkatalog. Zu weiteren Informationen über die Datenauswahl siehe daher 'Datenkatalog (S. 116)'.

Daten in der Archiv-Anzeige auswählen

1. Erweitern Sie das gewünschte Archiv und wählen Sie dann eines der aufeinander folgenden Backups anhand seines Zeitstempels. Auf diese Weise können Sie die Daten der Festplatte auf einen bestimmten Zeitpunkt zurücksetzen.

   Sollte die Liste der Archive nicht angezeigt werden (weil beispielsweise die Archiv-Metadaten verloren gingen), dann klicken Sie auf **Aktualisieren**.

   Falls die Liste der Archive zu lang ist, können Sie diese filtern, indem Sie festlegen, dass nur ein gewünschter Typ von Archiven angezeigt werden soll. Wählen Sie dazu den gewünschten Archivtyp in der Liste **Anzeigen**.
2. Nur für Laufwerk- oder Volume-Backups: Bestimmen Sie unter **Backup-Inhalt** den darzustellenden Datentyp aus dem Listenfeld:
   - **Laufwerke** – zur Wiederherstellung kompletter Laufwerke (mit all ihren Volumes).
   - **Volumes** – zur Wiederherstellung einzelner Volumes vom Typ 'Basis' oder 'Dynamisch'.
   - **Dateien** – zur Wiederherstellung einzelner Dateien und Ordner.
3. Aktivieren Sie bei **Backup-Inhalt** die Kontrollkästchen der Elemente, die Sie wiederherstellen müssen.
4. Klicken Sie auf **OK**.

MBR wählen

Sie wählen bei Wiederherstellung eines System-Volumes den MBR des Laufwerks üblicherweise dann, wenn:

- Das Betriebssystem nicht booten kann.
- Das Laufwerk neu ist und keinen MBR hat.
- Sie benutzerdefinierte oder Nicht-Windows-Boot-Loader (wie LILO und GRUB) wiederherstellen.
- Die Laufwerksgeometrie von der im Backup gespeicherten abweicht.

Es gibt vermutlich noch andere Situationen, bei denen Sie den MBR wiederherstellen müssen, aber die oberen sind die häufigsten.

Bei Wiederherstellung eines MBR von einem auf ein anderes Laufwerk stellt Acronis Backup auch Track 0 (Spur Null) wieder her, was keinen Einfluss auf die Partitionstabelle und das Partitionslayout des Ziellaufwerks hat. Acronis Backup aktualisiert nach einer Wiederherstellung automatisch die Windows Boot-Loader, daher ist es bei Windows-Systemen nicht notwendig, den MBR und Track 0 wiederherzustellen, außer der MBR ist beschädigt.

5.1.1.1 Speicherort für Archive wählen

Speicherort	Details
Cloud Storage	Falls das Archiv im Acronis Cloud Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben Sie anschließend die Anmeldedaten zum Zugriff auf den Cloud Storage ein. Erweitern Sie dann die Gruppe **Cloud Storage** und wählen Sie das Konto. *Im Acronis Cloud Storage gespeicherte Backups können nicht exportiert oder gemountet werden.*
Persönlich	Falls das Archiv in einem persönlichen Depot gespeichert ist, dann erweitern Sie die Gruppe **Persönlich** und klicken Sie auf das entsprechende Depot.
Maschinenname	Lokale Maschine
Lokale Ordner	Sollte das Archiv in einem lokalen Ordner auf der Maschine gespeichert sein, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Verzeichnis.
CD, DVD, BD	Falls das Archiv auf optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) gespeichert ist, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Laufwerk aus. Legen Sie zuerst den letzten Datenträger ein. Legen Sie die Medien dann nach Anforderung des Programms nacheinander ein, beginnend mit dem ersten Medium.
RDX, USB	Falls das Archiv auf einem RDX- oder USB-Flash-Laufwerk gesichert ist, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Laufwerk aus. Weitere Informationen über die Verwendung dieser Laufwerke finden Sie im Abschnitt 'Wechsellaufwerke (S. 170)'.
Bandgerät	Falls die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, dann erweitern Sie die Gruppe **Bandgeräte** und klicken Sie dann auf das benötigte Gerät. Bandgeräte stehen nur dann zur Verfügung, falls Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgeräte' in der Produkthilfe.
Netzwerkordner	Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

Speicherort	Details
FTP, SFTP	Sollte das Archiv auf einem FTP- oder SFTP-Server gespeichert sein, dann geben Sie den Namen oder die Adresse des Servers folgendermaßen in das Feld **Pfad** ein: **ftp://ftp-server:port-nummer oder sftp://sftp-server:port-nummer** Verwenden Sie folgende Schreibweise, um eine FTP-Verbindung im aktiven Modus aufzubauen: **aftp://ftp-server:port-nummer** Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP. Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server. Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten. *Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.*

5.1.1.2 Datenkatalog

Der Datenkatalog ermöglicht Ihnen, die benötigten Versionen bestimmter Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen. Auf einer verwalteten Maschine ist die Datenkatalogfunktionalität für jedes Depot, auf das von dieser Maschine zugegriffen werden kann, über die Registerlasche **Datenanzeige** verfügbar.

Acronis Backup lädt unter Umständen Datenkatalogdateien von einem Depot in einen lokalen Cache-Ordner. Dieser Ordner befindet sich standardmäßig auf dem Laufwerk, auf dem auch das Betriebssystem installiert ist. Informationen zur Änderung des vorgegebenen Cache-Ordners finden Sie im Abschnitt 'Den Standard-Cache-Ordner für Katalogdateien ändern'.

Gespeicherte Daten für eine Recovery-Aktion auswählen

1. Um auf die Registerkarte **Datenanzeige** zugreifen zu können, navigieren Sie zur Anzeige **Depots** und klicken Sie dort auf das erforderliche Depot.
2. Bestimmen Sie im Feld **Anzeigen** den darzustellenden Datentyp:
   - Wählen Sie **Maschinen/Laufwerke/Volumes**, um vorliegende laufwerkbasierte Backups nach kompletten Laufwerken und Volumes durchsuchen zu können.
   - Wählen Sie **Dateien/Ordner**, um vorliegende Datei- und Laufwerk-Backups nach Dateien und Ordnern durchsuchen zu können.
3. Spezifizieren Sie im Feld **Backups anzeigen für** den gewünschten Zeitraum, für den die gespeicherten Daten angezeigt werden sollen.
4. Wählen Sie aus den nachfolgenden Varianten:
   - Wählen Sie die wiederherzustellenden Daten aus dem Katalogverzeichnis oder in der rechts neben diesem liegenden Tabelle.
   - Binden Sie diejenigen Informationen in den Suchbegriff mit ein, die Ihnen helfen, die benötigten Datenelemente (das kann ein Maschinenname, ein Ordnername oder eine Laufwerksbezeichnung sein) zu identifizieren – und klicken Sie dann auf den Befehl **Suchen**. Sie können die Wildcards Sternchen (*) und Fragezeichen (?) verwenden.

     Als Ergebnis sehen Sie im Fenster **Suchen** eine Liste mit all den gespeicherten Datenelementen, deren Namen vollständig oder teilweise mit dem eingegebenen Wert

übereinstimmt. Sollte die Liste der Suchtreffer zu lang sein, dann können Sie die Suchkriterien verfeinern, beispielsweise indem Sie Datum bzw. Zeit der Backup-Erstellung und/oder einen Größenbereich für die gespeicherten Elemente angeben. Wenn die benötigten Daten gefunden sind, wählen Sie diese aus und klicken Sie dann auf **OK**, um zurück zur **Datenanzeige** zu gelangen.

5. Verwenden Sie die Liste der **Versionen**, um den Zeitpunkt zu bestimmen, zu dem hin die Daten wiederhergestellt werden sollen. Standardmäßig werden die Daten auf den jüngsten Zeitpunkt zurückgesetzt, der für den im Schritt 3 gewählten Zeitraum verfügbar ist.
6. Klicken Sie nach Auswahl der benötigten Daten auf **Recovery** und konfigurieren Sie dann die Parameter für die Wiederherstellungsaktion.

Was, wenn die Daten nicht in der Datenanzeige erscheinen?

Die wahrscheinlichen Gründe für dieses Problem sind:

Es wurde ein falscher Zeitraum eingestellt

Die benötigten Daten wurden während des Zeitraums, der über den Befehl **Backups anzeigen für** eingestellt wurde, nicht als Backup gesichert.

Lösung: Versuchen Sie, den Zeitraum zu vergrößern.

Katalogisierung ist deaktiviert oder die schnelle Katalogisierung ist angeschaltet

Falls die Daten nur teilweise oder überhaupt nicht angezeigt werden, war vermutlich die Katalogisierung deaktiviert oder während des Backups die schnelle Katalogisierung (S. 91) eingeschaltet.

Lösungen:

- Sollte die Katalogisierung deaktiviert sein, dann aktivieren Sie sie mit der Option **Backup-Katalogisierung** (**Optionen** –> **Maschinen-Optionen**).
- Führen Sie die vollständige Katalogisierung manuell aus, indem Sie auf **Jetzt katalogisieren** klicken. Für die **Datenanzeige** werden nur die auf dem gewählten Depot gespeicherten Backups katalogisiert. Zuvor bereits katalogisierte Backups werden nicht erneut katalogisiert.
- Da die Katalogisierung einer großen Anzahl an gespeicherten Daten längere Zeit benötigen kann, können Sie auf Wunsch auch die **Archiv-Anzeige** des entsprechenden Depots verwenden. Zu weiteren Informationen über die Verwendung der **Archiv-Anzeige** siehe den Punkt 'Depot-Inhalte durchsuchen und Datenauswahl' im Abschnitt 'Mit Depots arbeiten (S. 163)'.

Nicht vom Katalog unterstützte Daten

Folgende Daten können nicht im Katalog oder der Datenanzeige dargestellt werden:

- Daten aus verschlüsselten und kennwortgeschützten Archiven.
- Daten, die als Backup auf Wechselmedien wie CDs, DVDs, BDs, Iomega REV, RDX oder USB-Geräten gespeichert wurden.
- Daten, die zum bzw. in den Acronis Cloud Storage gesichert wurden.
- Daten, die mit Acronis True Image Echo oder früheren Versionen gesichert wurden.
- Daten, die mit vereinfachter Dateibenennung gesichert wurden.

Lösung: Verwenden Sie die Registerlasche **Archiv-Anzeige** des entsprechenden Depots, um solche Daten durchsuchen zu können.

5.1.2 Anmeldedaten für den Speicherort

Spezifizieren Sie die Anmeldedaten, die notwendig sind, um auf den Ort zuzugreifen, wo die Backups gespeichert sind.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Die Software greift auf den Speicherort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Die Software greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

5.1.3 Anmeldedaten für das Ziel

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Zielort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf den Zielort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Tasks keine Zugriffserlaubnis für den Zielort hat.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

5.1.4 Recovery-Ziel

Spezifizieren Sie das Ziel, auf dem die gewählten Daten wiederhergestellt werden sollen.

5.1.4.1 Ziellaufwerke wählen

Die als Ziel verfügbaren Laufwerke oder Volumes hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery zu:

Physikalische Maschine

Ist verfügbar, wenn der Acronis Backup Agent für Windows oder Agent für Linux installiert ist.

Die gewählten Laufwerke werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Neue virtuelle Maschine

- *Falls der Acronis Backup Agent für Windows oder der Agent für Linux installiert ist.*

  Die ausgewählten Laufwerke werden zu einer neuen virtuellen Maschine wiederhergestellt, die einem der folgenden Typen entspricht: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM), Red Hat Enterprise Virtualization (RHEV) oder Citrix XenServer Open Virtual Appliance (OVA).

  Die Dateien der virtuellen Maschine werden zu dem Ziel gespeichert, welches Sie im Bereich **Storage** spezifizieren. Die neue virtuelle Maschine wird standardmäßig im persönlichen Ordner für Dokumente des aktuellen Benutzers erstellt.
- *Falls der Acronis Backup Agent für Hyper-V oder der Agent für VMware installiert ist.*

  Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungsserver zu erstellen.

  Die neue virtuelle Maschine wird standardmäßig im Standard-Storage des Virtualisierungsservers erstellt. Ob Sie den Speicherort auf dem Virtualisierungsserver verändern können oder nicht, hängt vom Fabrikat und den Einstellungen des Virtualisierungsprodukts ab. VMware ESX(i) kann mehrere Speicherorte haben. Ein Microsoft Hyper-V-Server ermöglicht das Erstellen einer neuen virtuellen Maschine in jedem lokalen Ordner.

Die neue virtuelle Maschine wird automatisch konfiguriert, sofern möglich wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine** (S. 159) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Ist verfügbar, wenn der Acronis Backup Agent für Hyper-V oder der Agent für VMware installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungsserver und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Option VM-Energieverwaltung, falls Sie es vorziehen, diese manuell auszuschalten.

Laufwerke/Volumes

Automatisch zuordnen

Acronis Backup versucht die gewählten Laufwerke den entsprechenden Ziellaufwerken so zuzuordnen, wie im Abschnitt 'Wie die automatische Zuordnung arbeitet (S. 121)' beschrieben. Sollten Sie mit dem Zuordnungsergebnis unzufrieden sein, dann können Sie die Laufwerke

manuell neu zuordnen. Dazu müssen Sie die Zuordnung der Laufwerke in umgekehrter Reihenfolge wieder aufheben, die Zuordnung des zuletzt zugeordneten Laufwerks sollte also zuerst aufgehoben werden. Führen Sie die manuelle Zuordnung der Laufwerke dann wie nachfolgend beschrieben durch.

Laufwerk Nr.:

Laufwerk Nr. (MODELL) (S. 120)

Bestimmten Sie für jedes Quelllaufwerk das entsprechende Ziellaufwerk.

NT-Signatur (S. 120)

Bestimmten Sie, auf welche Art die wiederhergestellte Disk-Signatur gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

Zielfestplatte

So spezifizieren Sie ein Ziellaufwerk:

1. Bestimmen Sie eine Festplatte, wohin Sie die gewählte Festplatte wiederhergestellt haben wollen. Der Platz der Zielfestplatte sollte mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf der Zielfestplatte gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

NT-Signatur

Die NT-Signatur ist ein spezieller Datensatz, die im MBR hinterlegt ist. Sie dient der eindeutigen Identifizierung eines Laufwerks für das Betriebssystem.

Bei Wiederherstellung eines Laufwerks mit einem System-Volume können Sie wählen, was mit der NT-Signatur des Ziellaufwerks gemacht werden soll. Spezifizieren Sie einen der folgenden Parameter:

- **Automatische Auswahl**

  Die Software bewahrt die NT-Signatur des Ziellaufwerks, falls es sich um dieselbe NT-Signatur wie die im Backup vorliegende handelt. (Also mit anderen Worten, wenn Sie das Laufwerk auf dasselbe Laufwerk wiederherstellen, das zuvor ins Backup gesichert wurde). Anderenfalls generiert die Software eine neue NT-Signatur für das Ziellaufwerk.

  Diese vorgegebene Auswahl wird für die meisten Fälle empfohlen. Verwenden Sie die folgenden Einstellungen nur, wenn Sie sie wirklich benötigen.

- **Neu erstellen**

  Acronis Backup generiert eine neue NT-Signatur für das Ziellaufwerk.

- **Aus dem Backup wiederherstellen**

  Acronis Backup wird die NT-Signatur des Ziellaufwerks mit derjenigen aus dem Laufwerk-Backup ersetzen.

  ***Anmerkung**: Sie sollten sich absolut sicher sein, dass keine der in dieser Maschine vorhandenen Laufwerke dieselbe NT-Signatur hat. Anderenfalls startet das Betriebssystem vom ersten Laufwerk, erkennt dabei die gleiche Signatur auf dem zweiten Laufwerk, erzeugt automatisch eine neue, eindeutige NT-Signatur und weist diese dem zweiten Laufwerk zu. Als Konsequenz verlieren darauf dann alle Volumes des zweiten Laufwerks ihre Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf diesem Laufwerk kann daher auch nicht mehr booten.*

  Eine Wiederherstellung der Disk-Signatur kann aus folgenden Gründen wünschenswert sein:

- Acronis Backup steuert die Planung von Tasks unter Verwendung der Signatur des Quelllaufwerks. Wenn Sie dieselbe Disk-Signatur wiederherstellen, müssen Sie bereits erzeugte Tasks nicht neu erstellen oder bearbeiten.
- Einige installierte Anwendungen verwenden eine Disk-Signatur zur Lizenzierung oder für andere Einsatzzwecke.
- Das ermöglicht es Ihnen, alle Systemwiederherstellungspunkte von Windows auf dem wiederhergestellten Laufwerk zu behalten.
- So stellen Sie VSS-Snapshots (VSS = virtueller Schattenkopie-Dienst) wieder her, die von der Windows Vista-Funktion 'Vorherige Versionen' verwendet werden.

- **Existierende erhalten**

  Das Programm lässt die NT-Signatur des Ziellaufwerks unberührt.

Wie die automatische Zuordnung arbeitet

Acronis Backup führt nur dann eine automatische Zuordnung der Laufwerke bzw. Volumes zu den Ziellaufwerken durch, wenn dabei die Bootfähigkeit des Systems bewahrt wird. Anderenfalls wird die automatische Zuordnung abgebrochen und Sie müssen die Laufwerke bzw. Volumes automatisch zuordnen.

Sie müssen die Volumes außerdem auch dann manuell zuordnen, wenn logische Linux-Volumes oder Linux Software RAID-Volumes (MD-Geräte) vorliegen. Zu weiteren Informationen über die Wiederherstellung von logischen Volumes und MD-Geräten siehe den Abschnitt 'MD-Geräte und logische Volumes wiederherstellen'

Die automatische Zuordnung (Mapping) läuft folgendermaßen ab.

1. Wenn ein Laufwerk oder Volume zu seinem ursprünglichen Speicherort wiederhergestellt wird, dann reproduziert der Zuordnungsprozess das ursprüngliche Laufwerks- bzw. Volume-Layout.

   Der 'ursprüngliche' Speicherort für das Laufwerk bzw. Volume bedeutet, dass es sich um exakt dasselbe Laufwerk oder Volume handeln muss, das per Backup gesichert wurde. Ein Volume wird nicht als 'ursprünglich' betrachtet, wenn es seit dem Backup hinsichtlich Größe, Speicherort oder anderen physikalischen Parametern geändert wurde. Änderungen beim Laufwerksbuchstaben oder der Bezeichnung hindern die Software jedoch nicht daran, das Volume korrekt zu erkennen.

2. Falls das Laufwerk oder Volume zu einem anderen Speicherort wiederhergestellt wird:
   - **Bei Wiederherstellung von Laufwerken**: Die Software überprüft die Ziellaufwerke auf Größe und Volumes. Ein Ziellaufwerk darf keine Volumes enthalten und seine Größe muss ausreichend sein, um das wiederherzustellende Laufwerk aufzunehmen. Noch nicht initialisierte Ziellaufwerke werden automatisch initialisiert.

     Falls die benötigten Laufwerke nicht gefunden werden können, müssen Sie die Laufwerke manuell zuordnen.
   - **Bei Wiederherstellung von Volumes**: Die Software überprüft die Ziellaufwerke auf 'nicht zugeordneten' Speicherplatz.

     Falls der 'nicht zugeordnete' Speicherplatz ausreicht, werden die Volumes 'wie vorliegend' wiederhergestellt.

     Falls der 'nicht zugeordnete' Speicherplatz auf den Ziellaufwerken kleiner als die Größe der wiederherzustellenden Volumes ist, dann werden die Volumes proportional so angepasst (durch Verringerung ihres freien Speicherplatzes), dass Sie auf den 'nicht zugeordneten' Speicherplatz passen. Falls die verkleinerten Volumes immer noch nicht auf den 'nicht zugeordneten' Speicherplatz passen, müssen Sie die Volumes manuell zuordnen.

5.1.4.2 Ziel-Volumes wählen

Die verfügbaren Ziele für Volumes hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery zu:

Physikalische Maschine

Ist verfügbar, wenn der Acronis Backup Agent für Windows oder Agent für Linux installiert ist.

Die gewählten Volumes (Partitionen) werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Neue virtuelle Maschine

- *Falls der Acronis Backup Agent für Windows oder der Agent für Linux installiert ist.*

  Die ausgewählten Volumes werden zu einer neuen virtuellen Maschine wiederhergestellt, die einem der folgenden Typen entspricht: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM), Red Hat Enterprise Virtualization (RHEV) oder Citrix XenServer Open Virtual Appliance (OVA).

  Die Dateien der virtuellen Maschine werden zu dem Ziel gespeichert, welches Sie im Bereich **Storage** spezifizieren. Die neue virtuelle Maschine wird standardmäßig im persönlichen Ordner für Dokumente des aktuellen Benutzers erstellt.
- *Falls der Acronis Backup Agent für Hyper-V oder der Agent für VMware installiert ist.*

  Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungsserver zu erstellen.

  Die neue virtuelle Maschine wird standardmäßig im Standard-Storage des Virtualisierungsservers erstellt. Ob Sie den Speicherort auf dem Virtualisierungsserver verändern können oder nicht, hängt vom Fabrikat und den Einstellungen des Virtualisierungsprodukts ab. VMware ESX(i) kann mehrere Speicherorte haben. Ein Microsoft Hyper-V-Server ermöglicht das Erstellen einer neuen virtuellen Maschine in jedem lokalen Ordner.

Die neue virtuelle Maschine wird automatisch konfiguriert, sofern möglich wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine** (S. 159) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Ist verfügbar, wenn der Acronis Backup Agent für Hyper-V oder der Agent für VMware installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungsserver und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Option VM-Energieverwaltung, falls Sie es vorziehen, diese manuell auszuschalten.

Laufwerke/Volumes

Automatisch zuordnen

Acronis Backup versucht die gewählten Volumes den entsprechenden Ziellaufwerken so zuzuordnen, wie im Abschnitt 'Wie die automatische Zuordnung arbeitet (S. 121)' beschrieben. Sollten Sie mit dem Zuordnungsergebnis unzufrieden sein, dann können Sie die Volumes manuell neu zuordnen. Dazu müssen Sie die Zuordnung der Volumes in umgekehrter Reihenfolge wieder

aufheben, die Zuordnung des zuletzt zugeordneten Volumes sollte also zuerst aufgehoben werden. Führen Sie die manuelle Zuordnung der Volumes dann wie nachfolgend beschrieben durch.

[Disk Nr.] MBR wiederherstellen auf: [wenn der Master Boot Record für die Wiederherstellung ausgewählt ist]

Laufwerk Nr. (S. 123)

Wählen Sie das Laufwerk, auf der der Master Boot Record wiederhergestellt wird.

NT-Signatur: (S. 120)

Bestimmen Sie, wie die Laufwerk-Signatur im MBR gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

[Laufwerk] [Buchstabe] wiederherstellen auf:

Laufwerk Nr. /Volume

Ordnen Sie nacheinander jedem Quell-Volume einem Volume des Ziellaufwerkes oder 'nicht zugeordnetem' Speicherplatz zu.

Größe: (S. 124)

[Optional] Ändern Sie Größe, Position oder andere Eigenschaften des wiederhergestellten Volumes.

MBR-Ziel

So spezifizieren Sie ein Ziellaufwerk:

1. Wählen Sie das Ziellaufwerk aus, auf dem Sie den MBR wiederherstellen möchten.
2. Klicken Sie auf **OK**.

Ziel für ein Volume

So spezifizieren Sie ein Ziel-Volume oder 'nicht zugeordneten' Speicherplatz

1. Bestimmen Sie ein Volume oder 'nicht zugeordneten' Speicherplatz, wohin Sie das gewählte Volume wiederherstellen wollen. Das Ziel-Volume bzw. der nicht zugeordnete Speicherplatz sollten mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf dem Ziel-Volume gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

Bei Verwendung bootfähiger Medien

Laufwerksbuchstaben, die unter Windows-basierten Boot-Medien zu sehen sind, können von der Art abweichen, wie Windows seine Laufwerke normalerweise identifiziert. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Rettungs-Utility dem Laufwerk E: entsprechen, welches Windows verwendet.

Achtung! Um auf der sicheren Seite zu sein, ist es ratsam, den jeweils verwendeten Volumes eindeutige Namen zuzuweisen.

Ein Linux-typisches bootfähiges Medium zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).

Volume-Eigenschaften ändern

Größe und Speicherort

Sie können bei Wiederherstellung eines Volumes auf ein Basis-Laufwerk vom Typ MBR das Volume in seiner Größe oder Lage verändern, indem Sie dessen Darstellung bzw. Ränder mit der Maus verschieben oder indem Sie korrespondierende Werte in die entsprechenden Felder eingeben. Durch Verwendung dieser Funktion können Sie den Speicherplatz zwischen den wiederherzustellenden Volumes aufteilen. In diesem Fall müssen Sie zuerst das Volume wiederherstellen, welches in seiner Größe reduziert werden soll.

Beachten Sie: *Volumes, die mit der Option 'Sektor-für-Sektor' gesichert wurden, können nicht in der Größe angepasst werden.*

Tipp: *Die Größe eines Volumes kann nicht verändert werden, wenn es aus einem Backup wiederhergestellt wird, das auf mehrere entfernbare Medien verteilt wurde. Um die Größe des Volumes zu ändern, kopieren Sie alle Teile des Backups an einen einzigen Speicherort auf einer Festplatte (oder ähnlichem Laufwerk).*

Typ

Ein Basis-Laufwerk vom Typ MBR kann bis zu vier primäre Volumes enthalten – oder bis zu drei primäre Volumes sowie ein bis mehrere logische Laufwerke. Das Programm wählt standardmäßig den ursprünglichen Typ des Volumes. Sie können diese Einstellung ändern (falls erforderlich).

- **Primär**. Die Informationen über primäre Volumes sind in der MBR-Partitionstabelle enthalten. Die meisten Betriebssysteme können nur von einem primären Volume auf dem ersten Laufwerk booten, zudem ist die Zahl primärer Volumes limitiert.

  Wählen Sie bei Wiederherstellung eines System-Volumes auf ein Basis-Laufwerk vom Typ MBR das Kontrollkästchen 'Aktiv'. Ein aktives Volume wird zum Starten eines Betriebssystems verwendet. Wenn Sie jedoch 'Aktiv' für ein Volume ohne installiertes Betriebssystem wählen, kann das die Maschine daran hindern, zu booten. Ein logisches Laufwerk oder ein dynamisches Volume kann nicht auf 'Aktiv' gesetzt werden.
- **Logisch**. Die Informationen über logische Volumes sind nicht im MBR, sondern in der erweiterten Partitionstabelle hinterlegt. Die Anzahl logischer Volumes auf einer Festplatte (oder ähnlichem Laufwerk) ist nicht limitiert. Ein logisches Volume kann nicht als 'Aktiv' gesetzt werden. Wenn Sie ein System-Volume auf ein anderes Laufwerk mit eigenen Volumes (Partitionen) und Betriebssystem wiederherstellen, benötigen Sie wahrscheinlich nur die entsprechenden Daten. In diesem Fall können Sie das Volume auch als logisches Laufwerk wiederherstellen, um lediglich auf seine Daten zuzugreifen.

Dateisystem

Standardmäßig erhalten wiederhergestellte Volumes dasselbe Dateisystem wie das ursprünglich gesicherte Volume. Falls benötigt, können Sie jedoch das Dateisystem des Volumes während der Recovery-Aktion ändern.

Acronis Backup kann folgende Dateisysteme zueinander konvertieren: FAT16 –> FAT32 und Ext2 –> Ext3. Für Volumes mit anderen nativen Dateisystemen ist diese Option nicht verfügbar.

Angenommen, Sie wollen ein Volume von einem alten FAT16-Laufwerk mit niedriger Kapazität auf einer neueren Festplatte wiederherstellen. FAT16 wäre nicht effektiv und es könnte unter Umständen auch unmöglich sein, dieses Dateisystem auf das neue Laufwerk zu übertragen. Hintergrund ist, dass FAT16 nur Volumes bis 4 GB unterstützt, daher können Sie ein 4 GB FAT16-Volume nicht ohne Änderung des Dateisystems auf ein Laufwerk wiederherstellen, welches

über dieser Begrenzung liegt. In diesem Fall wäre es sinnvoll, das Dateisystem von FAT16 zu FAT32 zu wechseln.

Ältere Betriebssysteme (MS-DOS, Windows 95 und Windows NT 3.x, 4.x) unterstützen jedoch kein FAT32 und sind daher nicht betriebsbereit, nachdem Sie das Volume wiederhergestellt und das Dateisystem geändert haben. Diese können normalerweise nur auf ein FAT16-Volume wiederhergestellt werden.

Alignment von Volumes (Partitionen)

Acronis Backup beseitigt die Fehlausrichtung (Misalignment) von Volumes automatisch – also Situationen, in denen Volume-Cluster nicht passend zu den Laufwerkssektoren ausgerichtet sind. Zu einem Misalignment kommt es, wenn ein Volume, das mit einem CHS-Adressschema (Cylinder/Head/Sector) erstellt wurde, auf ein Laufwerk (Festplatte oder SSD) wiederhergestellt wird, welches eine Sektorgröße von 4 KB nutzt. Das CHS-Adressschema wird beispielsweise von allen Windows-Betriebssystemen vor Windows Vista verwendet.

Wenn bei Volumes ein Misalignment vorliegt, überlappen die Cluster mehr physikalische Sektoren, als es bei korrektem Alignment der Fall wäre. Als Folge müssen bei jeder Datenänderung mehr physikalische Sektoren als eigentlich nötig gelöscht und überschrieben werden. Diese unnötigen Lese-/Schreib-Operationen verringern spürbar die Laufwerksgeschwindigkeit (und damit auch die Gesamt-Performance des Systems). Ein Misalignment bei SSDs (Solid State Drives) verringert nicht nur die Performance des Systems bzw. Laufwerks, sondern auch dessen Lebensdauer. Da die Speicherzellen von SSDs nur auf eine bestimmte Menge von Lese-/Schreib-Operationen ausgelegt sind, führen redundante Lese-/Schreib-Operationen daher zu einem vorschnellen Verschleiß des SSD-Laufwerks.

Bei der Wiederherstellung von dynamischen Volumes und von logischen Volumes, die unter Linux mit dem Logical Volume Manager (LVM) erstellt wurden, wird das passende Alignment automatisch eingestellt.

Bei der Wiederherstellung von Basis-Volumes des Typs 'MBR' und 'GPT' können Sie die Alignment-Methode manuell wählen, sofern Sie das automatische Alignment aus irgendwelchen Gründen nicht zufriedenstellt. Folgende Optionen sind verfügbar:

- **Automatische Auswahl** – (Standard) empfohlen. Die Software stellt das passende Alignment automatisch ein, basierend auf den Laufwerk- bzw. Volume-Eigenschaften von Quelle und Ziel.

  Verwenden Sie die folgenden Optionen nur, wenn Sie sie wirklich benötigen.

  - **CHS (63 Sektoren)** – wählen Sie diese Option, wenn das wiederherzustellende Volume unter Windows XP oder Windows Server 2003 (oder früher) mit Laufwerken verwendet werden soll, die 512 Byte pro physikalischen Sektor haben.
  - **VMware VMFS (64 KB)** – wählen Sie diese Option, wenn Sie das Volume als eine 'VMware Virtual Machine File System'-Partition wiederherstellen wollen.
  - **Vista-Alignment (1 MB)** – wählen Sie diese Option, wenn das wiederherzustellende Volume unter Windows-Betriebssystemen ab Windows Vista (aufwärts) verwendet werden soll – oder wenn Sie das Volume auf ein Festplatten- oder SSD-Laufwerk wiederherstellen wollen, das eine Sektorgröße von 4 KB hat.
  - **Benutzerdefiniert** – spezifizieren Sie das Volume-Alignment manuell. Es wird empfohlen, dass der Wert ein Vielfaches der physikalischen Sektorgröße ist.

Logische Laufwerksbuchstaben (nur für Windows)

Standardmäßig wird dem Volume der erste freie Buchstabe zugewiesen. Wenn Sie einen anderen Laufwerksbuchstaben zuweisen wollen, dann wählen Sie einen entsprechenden aus dem Listenfeld.

Falls Sie den leeren Eintrag wählen, wird dem wiederhergestellten Volume kein Laufwerksbuchstabe zugewiesen und es so vor dem Betriebssystem verborgen. Sie sollten keine Laufwerksbuchstaben für Volumes vergeben, auf die Windows nicht zugreifen kann, beispielsweise bei Volumes, die kein FAT oder NTFS als Dateisystem verwenden.

5.1.4.3 Zielspeicherort für Dateien und Ordner wählen

Recovery-Ziel

Ziel

Wählen Sie einen Speicherort, in den die gesicherten Dateien wiederhergestellt werden:

- **Ursprünglicher Speicherort**

  Die Dateien und Ordner werden zu demselben Pfad(en) wiederhergestellt, wie sie im Backup vorliegen. Falls Sie z.B. alle Dateien und Ordner aus *C:\Dokumente\Finanzen\Berichte* gesichert hatten, so werden die Daten zu genau diesem Pfad wiederhergestellt. Sollte der Ordner nicht existieren, dann wird er automatisch erstellt.

- **Neuer Speicherort**

  Die Dateien werden zu dem Speicherort wiederhergestellt, den Sie im Verzeichnisbaum spezifizieren. Dabei werden die Dateien und Ordner ohne Anlegen eines vollständigen Pfades zurückgesichert, es sei denn, Sie deaktivieren das Kontrollkästchen **Ohne absolute Pfade wiederherstellen**.

Überschreiben

Bestimmen Sie, was geschehen soll, wenn das Programm im Zielordner eine Datei gleichen Namens wie im Archiv findet:

- **Existierende Dateien überschreiben** – dies gibt der Datei im Backup eine höhere Priorität als der Datei auf dem Ziellaufwerk.
- **Existierende Datei überschreiben, wenn sie älter ist** – Dateien mit den jüngsten Veränderungen erhalten Priorität, egal ob sie im Backup oder auf dem Laufwerk sind.
- **Existierende Dateien nicht überschreiben** – dies gibt der Datei auf dem Ziellaufwerk eine höhere Priorität als der Datei im Backup.

Falls Sie ein Überschreiben von Dateien erlauben, haben Sie dennoch die Option, spezielle Dateien davor zu schützen, nämlich indem Sie diese von der Recovery-Aktion ausschließen.

Ausschließungen vom Recovery (S. 126)

Spezifizieren Sie die Dateien und Ordner, die nicht wiederhergestellt werden sollen.

Ausschließungen vom Recovery

Richten Sie Ausschlusskriterien für spezielle Dateien und Ordner ein, die sie nicht wiederherstellen wollen.

***Hinweis:** Ausschließungen überschreiben eine Auswahl von wiederherzustellenden Datenelementen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' wiederhergestellt werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht wiederhergestellt.*

Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der auszuschließenden Dateien und Ordner zu verwalten. Spezifizieren Sie den Namen der Datei oder des Ordners, wie etwa 'Dokument.txt'.

Bei den Namen wird *nicht* auf Groß-/Kleinschreibung geachtet (in Windows und Linux). Falls Sie beispielsweise festlegen, dass alle .tmp-Dateien und Temp-Ordner ausgeschlossen werden sollen, dann werden auch alle .Tmp-Dateien, alle .TMP-Dateien und alle TEMP-Ordner ausgeschlossen.

Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden:

- Das Asterisk (*) ersetzt null bis mehrere Zeichen. So beinhaltet beispielsweise 'Doc*.txt' Dateien wie 'Doc.txt' und 'Document.txt'.
- Das Fragezeichen (?) steht für exakt ein Zeichen. Beispielsweise beinhaltet 'Doc?.txt' Dateien wie 'Doc1.txt' und 'Docs.txt' – aber nicht 'Doc.txt' oder 'Doc11.txt'.

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
Per Name	F.log F	Schließt alle Dateien namens 'F.log' aus Schließt alle Ordner namens 'F' aus
Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen

5.1.5 Recovery-Zeitpunkt

Bestimmen Sie, wann der Recovery-Task beginnen soll:

- **Jetzt** – der Recovery-Task wird direkt gestartet, sobald Sie auf der Seite **Daten wiederherstellen** auf **OK** klicken.
- **Später** – der Recovery-Tasks wird später manuell gestartet. Falls Sie eine Planung für den Task erstellen müssen, dann deaktivieren Sie das Kontrollkästchen **Task wird manuell gestartet** und spezifizieren Sie den gewünschten Zeitpunkt.

5.1.6 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten verwenden**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf 'OK'.

Weitere Informationen über die Verwendung von Anmeldedaten in Acronis Backup finden Sie im Abschnitt 'In Backup-Plänen und Tasks verwendete Anmeldedaten (S. 23)'.

Siehe den Abschnitt 'Benutzerberechtigungen auf einer verwalteten Maschine (S. 25)', um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

5.2 Acronis Universal Restore

Acronis Universal Restore ist eine proprietäre Acronis-Technologie, die Ihnen hilft, ein Betriebssystem auf abweichender Hardware oder einer virtuellen Maschine wiederherzustellen und zu booten. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

Universal Restore ist bei folgenden Szenarien besonders nützlich:

1. Sofortige Wiederherstellung eines ausgefallenen Systems auf abweichender Hardware.
2. Hardware-unabhängiges Klonen und Deployment von Betriebssystemen.
3. Migration von Maschinen von physikalisch zu physikalisch, physikalisch zu virtuell und virtuell zu physikalisch.

5.2.1 Universal Restore erwerben

Universal Restore ist in allen Acronis-Produkten enthalten, die Backups auf Laufwerksebene oder Single-Pass-Backups ermöglichen.

5.2.2 Universal Restore verwenden

Während einer Wiederherstellung

Universal Restore ist verfügbar, wenn Sie ein Laufwerk oder Volume wiederherstellen und dabei ein Windows- oder Linux-Betriebssystem in der Auswahl Ihrer Laufwerke bzw. Volumes enthalten ist. Sollte Ihre Auswahl mehr als ein Betriebssystem beinhalten, können Sie Universal Restore entweder auf alle Windows-Systeme, alle Linux-Systeme oder beide Systeme zusammen anwenden.

Falls die Software nicht erkennen kann, ob in dem Backup ein Betriebssystem vorhanden ist, schlägt sie die Verwendung von Universal Restore aufs Geratewohl für den Fall vor, dass ein System vorhanden ist. Diese Fälle sind wie folgt:

- Das Backup ist in mehrere Dateien aufgeteilt
- Das Backup befindet sich auf dem Acronis Cloud Storage, einem FTP-/SFTP-Server, auf Band, CD oder DVD.

Universal Restore ist nicht verfügbar, wenn:

- das Backup in der Acronis Secure Zone liegt
- Sie die Verwendung von Acronis Active Restore (S. 293) gewählt haben,

Und zwar weil alle diese Funktionen in erster Linie zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Ohne Wiederherstellung

Sie können Universal Restore auch unter einem bootfähigen Medium ohne Recovery-Aktion verwenden, indem Sie in der Willkommenseite des Mediums auf den Befehl **Universal Restore**

anwenden klicken. Universal Restore wird auf das Betriebssystem angewendet, das bereits auf der Maschine existiert. Falls es mehrere Betriebssysteme gibt, werden Sie aufgefordert, dasjenige zu wählen, auf das Universal Restore angewendet werden soll.

5.2.2.1 Universal Restore in Windows

Vorbereitung

Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie für den neuen Festplatten-Controller und Chipsatz die passenden Treiber haben. Diese Treiber sind für den Start des Betriebssystems entscheidend. Verwenden Sie die vom Hardware-Hersteller mitgelieferte CD bzw. DVD oder laden Sie die Treiber von der Website des Herstellers herunter. Die Treiber sollten die Erweiterungen *.inf, *.sys oder *.oem haben. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, dann extrahieren Sie diese unter Verwendung einer Dritthersteller-Anwendung.

Ein optimaler Ansatz ist es, die Treiber für die in Ihrer Organisation verwendete Hardware an einem Aufbewahrungsort zu speichern, sortiert nach Gerätetyp oder Hardware-Konfiguration. Sie können eine Kopie des Aufbewahrungsortes auf einer DVD oder einem USB-Stick vorhalten; verwenden Sie einige Treiber und fügen Sie diese den bootfähigen Medien hinzu; erstellen Sie für jeden Ihrer Server ein benutzerdefiniertes bootfähiges Medium mit den notwendigen Treibern (und der notwendigen Netzwerk-Konfiguration). Alternativ können Sie auch einfach jedes Mal, wenn Universal Restore verwendet wird, den Pfad zum Aufbewahrungsort angeben.

Überprüfen Sie den Zugriff auf die Treiber innerhalb der bootfähigen Notfallumgebung.

Stellen Sie sicher, dass Sie bei Verwendung eines bootfähigen Mediums auf das Gerät mit den Treibern zugreifen können. Sogar, wenn Sie eine Wiederherstellung des Systemlaufwerks unter Windows konfigurieren, wird die Maschine neu gestartet und die Recovery-Aktion dann in einer Linux-basierten Umgebung durchgeführt. Verwenden Sie ein WinPE-basiertes Medium, falls das Gerät unter Windows verfügbar ist, aber von einem Linux-basierten Notfallmedium nicht erkannt wird.

Was, wenn Sie keine Treiber haben?

Windows 7 enthält mehr Treiber als die früheren Windows-Betriebssysteme. Es besteht daher eine gute Chance, dass Universal Restore alle benötigten Treiber im Treiberordner von Windows 7 findet. Sie müssen also nicht unbedingt externe Pfade zu den Treibern angeben. Nichtsdestotrotz ist die Durchführung von Universal Restore kritisch, so dass das System die korrekten Treiber verwenden sollte.

*Der Standardordner von Windows zum Speichern von Treibern ist im Registry-Wert **DevicePath** hinterlegt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Normalerweise lautet dieser Speicherordner „WINDOWS/inf“.*

Universal Restore-Einstellungen

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für Hardware Abstraction Layer (HAL), Festplatten-Controller und Netzwerkadapter suchen soll:

- Befinden sich die Treiber auf einer Disc (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Während der Wiederherstellung führt Universal Restore eine rekursive Suche in allen Unterordnern des angegebenen Verzeichnisses durch, findet aus allen verfügbaren die am besten passenden HAL- und Festplatten-Controller-Treiber heraus und installiert diese in das wiederhergestellte System. Universal Restore sucht außerdem nach Treibern für Netzwerkadapter, der Pfad des gefundenen Treibers wird dann dem Betriebssystem durch Universal Restore übermittelt. Wenn die Hardware über mehrere Netzwerkkarten verfügt, so versucht Universal Restore, die Treiber aller Karten zu konfigurieren.

Auf jeden Fall zu installierende Massenspeichertreiber

Erweitern Sie zum Zugriff auf diese Einstellung den Punkt **Auf jeden Fall zu installierende Massenspeichertreiber**.

Sie benötigen diese Einstellung falls:

- Die Ziel-Hardware einen speziellen Massenspeicher-Controller wie RAID (insbesondere NVIDIA RAID) oder einen Fibre Channel-Adapter verwendet.
- Sie ein System zu einer virtuellen Maschine wiederherstellen, die einen SCSI-Festplatten-Controller verwendet und mit einem bootfähigen Medium gestartet wird. Verwenden Sie die SCSI-Treiber, die mit der Software für Ihre virtuellen Maschinen ausgeliefert werden – oder laden Sie die neueste Treiberversion von der Website des Software-Herstellers herunter.
- Die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Die hier angegebenen Treiber werden auch dann – unter entsprechenden Warnmeldungen – installiert, wenn das Programm einen besseren Treiber findet.

Der Recovery-Prozess

Falls Universal Restore an den angegebenen Speicherorten keinen kompatiblen Treiber finden kann, zeigt es zu dem Problemgerät eine Eingabeaufforderung an. Wählen Sie aus den nachfolgenden Varianten:

- Fügen Sie den Treiber einem der zuvor spezifizierten Speicherorte hinzu und klicken Sie auf **Wiederholen**.
- Wenn Sie sich nicht an den Speicherort erinnern, dann setzen Sie die Recovery-Aktion fort. Sollte das Ergebnis nicht zufriedenstellend sein, dann starten Sie Universal Restore ohne Recovery-Aktion, indem Sie in der Willkommenseite des Mediums auf den Befehl **Universal Restore anwenden** klicken. Spezifizieren Sie bei Konfiguration der Aktion den benötigten Treiber.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für den Netzwerkadapter wird ohne weitere Nachfrage installiert, sofern er eine Microsoft Windows-Signatur hat. Anderenfalls erfragt Windows Ihre Bestätigung zur Installation des unsignierten Treibers.

Danach können Sie die Netzwerk-Verbindung konfigurieren und Treiber für Grafikkarte, USB- und andere Geräte spezifizieren.

5.2.2.2 Universal Restore auf mehrere Betriebssysteme anwenden

Sie können Universal Restore während einer Recovery-Aktion für Betriebssysteme eines bestimmten Typs verwenden: alle Windows-Systeme, alle Linux-Systeme oder beide.

Falls Ihre Auswahl der wiederherzustellenden Volumes mehrere Windows-Systeme enthält, können Sie alle für diese gedachten Treiber in einer einzigen Liste spezifizieren. Jeder Treiber wird in das jeweilige Betriebssystem installiert, für das er vorgesehen ist.

5.3 Recovery von BIOS-basierten Systemen zu UEFI-basierten Systemen und umgekehrt

Acronis Backup unterstützt die Übertragung von 64-Bit-Windows-Betriebssystemen zwischen BIOS-basierter Hardware und Hardware, die 'Unified Extensible Firmware Interface' (UEFI) unterstützt.

Die Funktionsweise

Abhängig davon, ob die Maschine eine BIOS- oder UEFI-Firmware zum Booten verwendet, muss das Laufwerk mit dem System-Volumen ein bestimmtes *Partitionierungsschema* haben. Das Partitionierungsschema ist MBR (Master Boot Record) beim BIOS-Standard und GPT (GUID Partition Table) beim UEFI-Standard.

Zusätzlich reagiert auch das Betriebssystem selbst auf den Typ der Firmware.

Bei Durchführung einer Wiederherstellung auf eine Maschine, deren Firmware sich von der der ursprünglichen Maschine unterscheidet, macht Acronis Backup Folgendes:

- Es initialisiert das Laufwerk, zu dem Sie das System-Volume wiederherstellen, entweder als MBR- oder als GPT-Laufwerk – abhängig von der neuen Firmware.
- Es passt das Windows-Betriebssystem so an, dass es von der neuen Firmware starten kann.

Weitere Details (einschließlich einer List von Windows-Betriebssystemen, die auf diese Art angepasst werden können) finden Sie unter 'Wiederherstellung von Volumes (S. 132)' und 'Wiederherstellung von Laufwerken (S. 133)' in diesem Abschnitt.

Empfehlungen

- Stellen Sie das komplette System auf nicht initialisierte Laufwerke wieder her.
- Verwenden Sie beim Migrieren auf bzw. zu einer UEFI-basierten Hardware ein Linux-basiertes oder WinPE-basiertes (höher als Version 4.0) Boot-Medium. Ältere Versionen von WinPE und dem Acronis PXE Server unterstützen kein UEFI.
- Beachten Sie, dass der BIOS-Standard es nicht erlaubt, Laufwerksspeicherplatz mit mehr als 2 TB zu verwenden.

Beschränkungen

Die Übertragung eines Linux-Systems zwischen UEFI und BIOS wird nicht unterstützt.

Die Übertragung eines Windows-Systems zwischen UEFI und BIOS wird nicht unterstützt, falls das Backup an einem dieser Speicherorte vorliegt:

- Acronis Cloud Storage
- Bandgerät
- Optische Datenträger (CDs, DVDs oder Blu-ray-Medien)

Sollte die Übertragung eines Systems zwischen UEFI und BIOS nicht unterstützt werden, dann initialisiert Acronis Backup das Ziellaufwerk mit demselben Partitionierungsschema wie das ursprüngliche Laufwerk. Dabei erfolgt keine Anpassung des Betriebssystems. Sollte die Zielmaschine sowohl UEFI wie auch BIOS unterstützen, dann müssen Sie noch den zur ursprünglichen Maschine passenden Boot-Mode aktivieren. Anderenfalls wird das System nicht mehr booten.

5.3.1 Volumes wiederherstellen

Angenommen, Sie haben ein Backup der System- und Boot-Volumes durchgeführt (oder der kompletten Maschine) und wollen diese Volumes nun zu einer anderen Plattform wiederherstellen. Die Fähigkeit des wiederhergestellten Systems zu booten, hängt von folgenden Faktoren ab:

- **Betriebssystem der Quelle:** ist das Betriebssystem konvertierbar oder nicht? Konvertierbare Betriebssystem erlauben es, den Boot-Modus von BIOS zu UEFI zu konvertieren (und zurück).
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme (beginnend mit Windows Vista x64 SP1) sind konvertierbar.
  - Die 64-Bit-Versionen aller Windows Server-Betriebssysteme (beginnend mit Windows Server 2008 x64 SP1) sind konvertierbar.

  Alle anderen Betriebssysteme sind nicht konvertierbar.
- **Partitionsschema von Quell- und Ziellaufwerk**: MBR oder GPT. Die System- und Boot-Volumes von BIOS-Plattformen verwenden MBR-Laufwerke. Die System- und Boot-Volumes von UEFI-Plattformen verwenden GPT-Laufwerke.

  Wenn Sie bei einer Wiederherstellung ein nicht initialisiertes Ziellaufwerks auswählen, wird das Laufwerk automatisch zu GPT oder MBR initialisiert – in Abhängigkeit vom Partitionsschema des ursprünglichen Laufwerks, dem aktuellen Boot-Modus (UEFI oder BIOS) und dem Typ der auf diesem Volume vorhandenen Betriebssysteme (konvertierbar oder 'nicht konvertierbar').

  Falls die Initialisierung zum Verlust der Bootfähigkeit führen kann, verwendet die Software – unter Ignorieren der Größe des Ziellaufwerks – das Partitionsschema des Quell-Volumes. In solchen Fällen kann die Software für Laufwerke, die größer als 2 TB sind, das MBR-Partitionierungsschema wählen – wobei der Speicherplatz oberhalb von 2 TB jedoch nicht nutzbar ist.

  Sie können das Ziellaufwerk bei Bedarf auch manuell initialisieren, indem Sie die Funktion zur Laufwerksverwaltung (S. 204) verwenden.

Die folgenden Tabelle fasst zusammen, ob die Bootfähigkeit eines Systems erhalten werden kann, wenn Sie Boot- und System-Volumes eines BIOS-basierten auf ein UEFI-basiertes System wiederherstellen (und umgekehrt).

- Ein grüner Hintergrund bedeutet, dass das System boofähig sein wird. Es ist kein Benutzereingriff erforderlich.
- Ein gelber Hintergrund bedeutet, dass Sie zusätzliche Schritte durchführen müssen, um das System bootfähig zu machen. Diese Schritte sind auf einigen Maschinen jedoch nicht möglich.
- Ein roter Hintergrund bedeutet, dass das System aufgrund von Beschränkungen der BIOS- bzw. UEFI-Plattform nicht bootfähig sein wird.

<table>
<tr><th rowspan="2">Ursprüngliches System</th><th colspan="4">Ziel-Hardware</th></tr>
<tr><td>BIOS
Laufwerk: MBR</td><td>BIOS
Laufwerk: GPT</td><td>UEFI
Laufwerk: MBR</td><td>UEFI
Laufwerk: GPT</td></tr>
<tr><td>BIOS
Betriebssystem: konvertierbar</td><td rowspan="2"></td><td rowspan="2">Lösung
Stellen Sie das Betriebssystem zu einem MBR-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td><td rowspan="2">Die Zielmaschine muss BIOS unterstützen.
Zusätzliche Schritte
1. Schalten Sie vor der Wiederherstellung den UEFI-Modus im BIOS aus
2. Führen Sie die Wiederherstellung mit einem bootfähigen Medium aus.
oder
Schalten Sie nach der Wiederherstellung den UEFI-Modus im BIOS aus.</td><td>Ein konvertierbares Betriebssystem wird automatisch zur Unterstützung von UEFI zum Booten konvertiert.</td></tr>
<tr><td>BIOS
Betriebssystem: nicht konvertierbar</td><td>Lösung
Stellen Sie das Betriebssystem zu einem MBR-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td></tr>
<tr><td>UEFI
Betriebssystem: konvertierbar</td><td>Ein konvertierbares Betriebssystem wird automatisch zur Unterstützung des BIOS-Modus zum Booten konvertiert.</td><td rowspan="2">Die Zielmaschine muss UEFI unterstützen.
Zusätzliche Schritte
1. Schalten Sie vor der Wiederherstellung den UEFI-Modus im BIOS an.
2. Führen Sie die Wiederherstellung mit einem bootfähigen Medium aus.
oder
Schalten Sie nach der Wiederherstellung den UEFI-Modus im BIOS an.</td><td rowspan="2">Lösung
Stellen Sie das Betriebssystem zu einem GPT-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td><td rowspan="2"></td></tr>
<tr><td>UEFI
Betriebssystem: nicht konvertierbar</td><td>Lösung
Stellen Sie das Betriebssystem zu einem GPT-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td></tr>
</table>

5.3.2 Laufwerke wiederherstellen

Angenommen, Sie haben ein komplettes Laufwerk (mit all seinen Volumes) per Backup gesichert und wollen nun dieses Laufwerk zu einer anderen Zielplattform wiederherstellen.

Die Fähigkeit des wiederhergestellten Systems, in verschiedenen Modi booten zu können, hängt von den auf dem Quelllaufwerk installierten Betriebssystemen ab. Betriebssysteme können **konvertierbar** sein, d.h. einen Wechsel des Boot-Modus von BIOS zu UEFI (und zurück) erlauben – oder eben **nicht konvertierbar** sein. Eine Liste konvertierbarer Betriebssysteme finden Sie unter 'Volumes wiederherstellen (S. 132)'.

- Wenn ein Quelllaufwerk ein oder mehrere Betriebssysteme enthält und *alle* davon konvertierbar sind, dann kann der Boot-Modus automatisch gewechselt werden. In Abhängigkeit vom aktuellen Boot-Modus wird das Ziellaufwerk möglicherweise entweder mit dem GPT- oder MBR-Partitionsschema initialisiert.
- Falls *mindestens ein* Betriebssystem auf dem Quelllaufwerk 'nicht konvertierbar' ist (oder das Quelllaufwerk ein Boot-Volume eines 'nicht konvertierbaren' Betriebssystems enthält), dann kann der Boot-Modus nicht automatisch gewechselt werden und wird die Software das Ziellaufwerk wie das Quelllaufwerk initialisieren. Um die Zielmaschine booten zu können, müssen Sie den UEFI-Modus im BIOS manuell ein- bzw. ausschalten. Anderenfalls wird das System nach der Wiederherstellung nicht mehr booten.

Die folgende Tabelle fasst alle Wiederherstellungsvarianten von Laufwerken eines BIOS-basierten zu einem UEFI-basierten System (und umgekehrt) zusammen.

- Ein grüner Hintergrund bedeutet, dass das System boofähig sein wird. Es ist kein Benutzereingriff erforderlich.
- Ein gelber Hintergrund bedeutet, dass Sie zusätzliche Schritte durchführen müssen, um das System bootfähig zu machen. Diese Schritte sind auf einigen Maschinen jedoch nicht möglich.

Ursprüngliches System	**Ziel-Hardware**	
	BIOS	UEFI
BIOS Betriebssystem: konvertierbar		Das Ziellaufwerk wird als GPT initialisiert. Das Betriebssystem wird automatisch zur Unterstützung von UEFI zum Booten konvertiert. Falls Sie das Quelllaufwerk 'wie vorliegend' wiederherstellen wollen: 1. Schalten Sie den UEFI-Modus im BIOS aus. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.
BIOS Betriebssystem: nicht konvertierbar		Das Ziellaufwerk wird wie das Quelllaufwerk initialisiert (MBR). *Die Zielmaschine muss BIOS unterstützen.* **Zusätzliche Schritte** 1. Schalten Sie den UEFI-Modus im BIOS aus. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.

Ursprüngliches System	Ziel-Hardware	
	BIOS	UEFI
UEFI Betriebssystem: konvertierbar	Das Ziellaufwerk wird als MBR initialisiert. Das Betriebssystem wird automatisch konvertiert, um das Booten per BIOS zu unterstützen. Falls Sie das Quelllaufwerk 'wie vorliegend' wiederherstellen wollen: 1. Schalten Sie den UEFI-Modus im BIOS ein. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.	
UEFI Betriebssystem: nicht konvertierbar	Das Ziellaufwerk wird wie das Quelllaufwerk initialisiert (GPT). *Die Zielmaschine muss UEFI unterstützen.* **Zusätzliche Schritte** 1. Schalten Sie den UEFI-Modus im BIOS ein. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.	

Wiederherstellung auf große Laufwerk in einem BIOS-System

Nach einer Wiederherstellung zu einem BIOS-basierten System wird das Zielsystemlaufwerk als MBR initialisiert. Aufgrund der Laufwerksgrößenbeschränkung im BIOS-Standard stehen für Laufwerke, die größer sind als 2 TB, nur die ersten 2 TB des Laufwerkspeicherplatzes zur Verfügung. Sollte die Maschine UEFI unterstützen, dann lässt sich diese Beschränkung umgehen, indem Sie den UEFI-Modus einschalten und dann die Wiederherstellung durchführen. Das Laufwerk wird nach dem GPT-Standard initialisiert. Bei GPT-Laufwerken existiert keine 2 TB-Beschränkung.

5.4 Acronis Active Restore

Active Restore ist eine geschützte Acronis-Technologie, die ein System direkt verfügbar macht, sobald dessen Wiederherstellung gestartet wurde.

Beschränkungen

- Active Restore ist nicht verfügbar, wenn Sie Windows 8/8.1 oder Windows Server 2012/2012 R2 wiederherstellen.
- Active Restore ist zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht. Bei Wiederherstellungen auf abweichende Hardware steht es nicht zur Verfügung.
- Der einzig unterstützte Archiv-Speicherort ist ein lokales Laufwerk oder, um präziser zu sein, jedes über das BIOS der Maschine ansprechbare Gerät. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.
- Active Restore unterstützt keine Laufwerke mit GPT-Partitionierungsschema bei Wiederherstellungsaktionen (weder als Quelle noch als Ziel) und auch nicht als

Archiv-Speicherort. Das bedeutet auch, dass UEFI (Unified Extensible Firmware Interface) nicht unterstützt wird. Der einzige unterstützte Boot-Modus ist BIOS.

Die Funktionsweise

Beim Konfigurieren einer Wiederherstellungsaktion wählen Sie die Laufwerke bzw. Volumes, um diese aus einem Backup wiederherzustellen. Acronis Backup scannt die gewählten, im Backup befindlichen Festplatten oder Laufwerke. Findet der Scan dabei ein unterstütztes Betriebssystem, so wird Acronis Active Restore verfügbar.

Sofern Sie Active Restore nicht aktivieren, erfolgt die Systemwiederherstellung auf die übliche Art und wird die Maschine erst nach vollständiger Wiederherstellung wieder einsatzbereit.

Falls Sie Active Restore aktivieren, wird die Sequenz der Aktionen folgendermaßen festgelegt:

Sobald die Systemwiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt.

Da die Bedienung solcher Anforderungen simultan zur Wiederherstellung erfolgt, kann das Betriebssystem ausgebremst werden – auch dann, wenn in den Recovery-Optionen die Recovery-Priorität (S. 149) auf **Niedrig** eingestellt wurde. Obwohl die Systemausfallzeit minimal ist, kann es während der Wiederherstellung zu einer verringerten Performance kommen.

Einsatzszenarien

1. Die Verfügbarkeit eines Systems gehört zu den Effizienzkriterien.

   Beispiele: Client-bezogene Online-Dienste, Web-Einzelhändler, Wahllokale

2. Das Verhältnis von System zu Speicherplatz ist stark in Richtung Speicher verzerrt.

   Einige Maschinen werden als Speicheranlagen genutzt, wobei das Betriebssystem nur ein kleines Speichersegment beansprucht, während der restliche Festplattenplatz der Archivierung dient, etwa für Videos, Audio- oder andere Multimedia-Dateien. Einige dieser Speicher-Laufwerke können verglichen zum System extrem groß sein, so dass praktisch die komplette Wiederherstellungszeit der Rückgewinnung der Dateien gewidmet wird, obwohl sie erst später gebraucht werden könnten (wenn in naher Zukunft überhaupt).

   Entscheiden Sie sich dagegen für Acronis Active Restore, so wird das System in kurzer Zeit wieder einsatzfähig sein. Benutzer werden in die Lage versetzt, benötigte Dateien aus dem Datenspeicher zu öffnen und zu verwenden, während alle restlichen, nicht sofort benötigten Dateien im Hintergrund weiter wiederhergestellt werden.

   Beispiele: Datenspeicher für Film- oder Musiksammlungen bzw. Multimedia-Dateien

Anwendung

1. Speichern Sie das Backup des Systemlaufwerks bzw. -volumes an einer Position, auf die über das System-BIOS zugegriffen werden kann. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.

   Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht mehr startet.

2. Erstellen Sie ein bootfähiges Medium.
3. Booten Sie die Maschine mit einem bootfähigen Medium, wenn es zu einem Systemausfall kommt. Starten Sie die Konsole und verbinden Sie sich mit dem bootfähigen Agenten.

4. Erstellen Sie einen Recovery-Task (S. 112). Stellen Sie bei **Recovery-Quelle** sicher, dass das System-Laufwerk oder System-Volume für die Wiederherstellung ausgewählt wurde.

   Acronis Active Restore wählt für das Hochfahren und die nachfolgende Wiederherstellung das erste beim Backup-Scan gefundene Betriebssystem. Versuchen Sie nicht, mehr als ein Betriebssystem unter Verwendung von Active Restore wiederherzustellen, damit die Ergebnisse berechenbar bleiben. Wählen Sie auch bei Wiederherstellung eines Multi-Boot-Systems nur jeweils ein System-Volume und Boot-Volume.

5. Stellen Sie bei **Recovery-Ziel** sicher, dass das System-Laufwerk oder System-Volume dem ersten Laufwerk zugeordnet ist. Sollte dem nicht so sein, dann führen Sie eine manuelle Zuordnung durch (wie im Abschnitt 'Ziellaufwerke wählen (S. 119)' beschrieben).
6. Wählen Sie bei **Acronis Active Restore** die Option **Verwenden**.
7. Sobald die Systemwiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Das Acronis Active Restore-Symbol erscheint im Infobereich der Taskleiste. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Ein das System sofort benutzender Anwender sieht den Verzeichnisbaum mit seinen Symbolen, kann Dateien öffnen oder Anwendungen starten, selbst wenn diese noch nicht wiederhergestellt wurden.

   Die Treiber von Acronis Active Restore fangen Systemanfragen ab und setzen Dateien, die zur Erfüllung einkommender Anfragen notwendig sind, auf höchste Wiederherstellungspriorität. Und während diese 'on-the-fly'-Wiederherstellung fortschreitet, wird der noch andauernde Wiederherstellungsprozess in den Hintergrund transferiert.

   Solange die Recovery-Aktion nicht abgeschlossen ist, sollten Sie nicht versuchen, die Maschine herunterzufahren oder einen Neustart durchzuführen. Falls Sie Ihr Maschine ausschalten, gehen alle seit dem letzten Systemstart durchgeführten Änderungen verloren. Das System wird dann nicht wiederhergestellt, auch nicht partiell. Die einzig verbliebene Lösung in diesem Fall ist es dann, den Wiederherstellungsprozess von einem bootfähigen Medium aus neu zu starten.

8. Die Hintergrund-Wiederherstellung geht solange weiter, bis alle gewählten Laufwerke wiederhergestellt wurden, alle Ereignismeldungen gemacht wurden und das Acronis Active Restore-Symbol aus dem Infobereich der Taskleiste verschwindet.

5.5 Troubleshooting zur Bootfähigkeit

Wenn ein System zum Zeitpunkt seines Backups bootfähig war, erwarten Sie auch, dass es nach einer Wiederherstellung booten kann. Informationen, die das Betriebssystem zum Booten speichert und verwendet, können jedoch bei einer Wiederherstellung ungültig werden, insbesondere, wenn Sie die Volume-Größe, die Speicherorte oder die Ziellaufwerke ändern. Acronis Backup aktualisiert Windows Boot-Loader automatisch nach einer Wiederherstellung. Auch andere Boot-Loader werden möglicherweise repariert, es gibt jedoch Fälle, bei denen Sie selbst die Loader reaktivieren müssen. Speziell, wenn Sie Linux-Volumes wiederherstellen, ist es manchmal notwendig, Fehlerkorrekturen anzuwenden oder Boot-Veränderungen durchzuführen, damit Linux korrekt startet und geladen werden kann.

Nachfolgend eine Zusammenfassung typischer Situationen, die zusätzliche Benutzereingriffe benötigen.

Warum ein wiederhergestelltes Betriebssystem nicht mehr bootfähig sein kann

- **Das BIOS der Maschine ist so konfiguriert, dass es von einem anderen Laufwerk bootet.**

  Lösung: Konfigurieren Sie das BIOS so, dass es von dem Laufwerk bootet, auf dem das Betriebssystem liegt.
- **Das System wurde auf abweichender Hardware wiederhergestellt und die neue Hardware ist inkompatibel mit den wichtigsten im Backup enthaltenen Treibern,**

Lösung: Starten Sie die Maschine mit einem bootfähigen Medium und wenden Sie Acronis Universal Restore an (S. 128), um die passenden Treiber und Module zu installieren.

- **Windows wurde zu einem dynamischen Volume wiederhergestellt, das nicht bootfähig sein kann.**

  Lösung: Führen Sie eine Wiederherstellung von Windows auf ein Volume vom Typ 'Basis', 'Einfach' oder 'Gespiegelt' durch.

- **Ein System-Volume wurde zu einem Laufwerk wiederhergestellt, das keinen MBR hat.**

  Wenn Sie die Wiederherstellung eines System-Volumes auf einem Laufwerk ohne MBR konfigurieren, fragt Sie das Programm, ob Sie zusammen mit dem System-Volume auch den MBR wiederherstellen wollen. Entscheiden Sie sich nur dann gegen eine Wiederherstellung, wenn Sie nicht wollen, dass das System bootfähig wird.

  Lösung: Stellen Sie das Volume zusammen mit dem MBR dem korrespondierenden Laufwerk wieder her.

- **Das System verwendet den Acronis OS Selector**

  Weil der Master Boot Record (MBR) während der System-Wiederherstellung ausgetauscht werden kann, ist es möglich, dass der Acronis OS Selector, der den MBR verwendet, funktionsunfähig wird. Reaktivieren Sie den Acronis OS Selector folgendermaßen, wenn dies passieren sollte:

  Lösung: Starten Sie die Maschine mit dem bootfähigen Medium des Acronis Disk Director und wählen Sie im Menü **Extras –> OS Selector aktivieren**.

- **Das System verwendet den GRand Unified Bootloader (GRUB) und wurde von einem normalen Backup (nicht 'Raw' bzw. Sektor-für-Sektor) wiederhergestellt.**

  Ein Teil des GRUB-Loaders liegt entweder in den ersten Sektoren des Laufwerks oder in den ersten Sektoren des Volumes. Der Rest befindet sich im Dateisystem einer der Volumes. Die Bootfähigkeit des Systems kann nur dann automatisch wiederhergestellt werden, wenn GRUB innerhalb der ersten Sektoren des Laufwerks sowie im Dateisystem liegt, zu dem ein direkter Zugriff möglich ist. In allen anderen Fällen muss der Benutzer den Boot-Loader manuell reaktivieren.

  Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen möglicherweise auch noch die Konfigurationsdatei reparieren.

- **Das System verwendet Linux Loader (LILO) und wurde von einem normalen Backup (nicht 'Raw' bzw. Sektor-für-Sektor) wiederhergestellt.**

  LILO enthält zahlreiche Verweise zu absoluten Sektor-Nummern und kann daher nicht automatisch repariert werden, außer wenn alle Daten genau zu denjenigen Sektoren wiederhergestellt werden, die dieselben absoluten Nummern wie auf dem Quelllaufwerk haben.

  Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen außerdem möglicherweise aus dem im vorherigen Punkt genannten Grund die Konfigurationsdatei des Loaders reparieren.

- **Der System-Loader verweist auf das falsche Volume**

  Dies kann passieren, wenn System- bzw. Boot-Volumes nicht zu ihrer ursprünglichen Position wiederhergestellt werden.

  Lösung: Für Windows-Loader wird dies durch eine Anpassung der Dateien 'boot.ini' bzw. 'boot/bcd' behoben. Acronis Backup führt dies automatisch durch und daher ist es unwahrscheinlich, dass Sie dieses Problem erleben.

  Für die Loader von GRUB und LILO müssen Sie die Konfigurationsdateien korrigieren. Hat sich die Nummer der Linux Root-Partition verändert, so ist es außerdem empfehlenswert, dass Sie '/etc/fstab' anpassen, damit korrekt auf das SWAP-Laufwerk zugegriffen werden kann.

- **Linux wurde von einem LVM-Volume-Backup auf ein Basis-MBR-Laufwerk wiederhergestellt.**

  Ein solches System kann nicht booten, weil sein Kernel versucht, das Root-Dateisystem von der LVM-Volume zu mounten.

  Lösung: Ändern Sie die Konfiguration des Loaders und '/etc/fstab' – so dass LVM nicht mehr verwendet wird – und reaktivieren Sie den Boot-Loader.

5.5.1 So reaktivieren Sie GRUB und ändern die Konfiguration

Für gewöhnlich sollten Sie die passende Prozedur in den Unterlagen zum Boot-Loader nachschlagen. Es gibt auch den entsprechenden Artikel in der Knowledge Base auf der Acronis-Website.

Nachfolgend ein Beispiel, wie Sie GRUB reaktivieren, wenn das Systemlaufwerk (Volume) auf identische Hardware wiederhergestellt wird.

1. Starten Sie Linux oder starten Sie von einem bootfähigen Medium und drücken Sie dann Strg+Alt+F2.
2. Mounten Sie das System, das Sie wiederherstellen:
   ```
   mkdir /mnt/system/
   mount -t ext3 /dev/sda2 /mnt/system/ # root partition
   mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot partition
   ```
3. Mounten Sie die Dateisysteme **proc** und **dev** an das wiederherzustellende System:
   ```
   mount -t proc none /mnt/system/proc/
   mount -o bind /dev/ /mnt/system/dev/
   ```
4. Sichern Sie eine Kopie der „menu“-Datei von GRUB, indem Sie einen der folgenden Befehle ausführen:
   ```
   cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
   ```
   oder
   ```
   cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
   ```
5. Bearbeiten Sie die Datei **/mnt/system/boot/grub/menu.lst** (für Debian-, Ubuntu- und SUSE Linux-Distributionen) oder die Datei **/mnt/system/boot/grub/grub.conf** (für Fedora- und Red Hat Enterprise Linux-Distributionen) — z.B. wie folgt:
   ```
   vi /mnt/system/boot/grub/menu.lst
   ```
6. Suchen Sie in der Datei **menu.lst** (alternativ **grub.conf**) den Menü-Eintrag, der zu dem von Ihnen wiederhergestellten System korrespondiert. Dieser Menü-Eintrag sieht folgendermaßen aus:
   ```
   title Red Hat Enterprise Linux Server (2.6.24.4)
         root (hd0,0)
         kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
         initrd /initrd-2.6.24.4.img
   ```
   Die Zeilen, die mit **title**, **root**, **kernel** bzw. **initrd** beginnen, legen Folgendes fest:
   - Den Titel des Menü-Eintrages.
   - Das Gerät, auf dem sich der Linux-Kernel befindet – üblicherweise die Boot- oder root-Partition, im vorliegenden Beispiel **root (hd0,0)**.
   - Der Pfad zum Kernel auf diesem Gerät und der root-Partition – im vorliegenden Beispiel ist der Pfad **/vmlinuz-2.6.24.4** und die root-Partition ist **/dev/sda2**. Sie können die root-Partition über ihre Bezeichnung (in der Form von **root=LABEL=/**), den Identifier (in der Form von **root=UUID=***some_uuid*) oder den Gerätenamen (**root=/dev/sda2**) spezifizieren.
   - Der Pfad zum Dienst **initrd** auf diesem Gerät.

7. Bearbeiten Sie die Datei **/mnt/system/etc/fstab**, um die Namen all der Geräte zu korrigieren, die sich als Ergebnis der Wiederherstellung verändert haben.
8. Starten Sie die Shell von GRUB, indem Sie einen der folgenden Befehle ausführen:

   ```
   chroot /mnt/system/ /sbin/grub
   ```

   oder

   ```
   chroot /mnt/system/ /usr/sbin/grub
   ```

9. Spezifizieren Sie das Laufwerk, auf dem sich GRUB befindet – üblicherweise die Boot- oder root-Partition.

   ```
   root (hd0,0)
   ```

10. Installieren Sie GRUB. Um GRUB z.B. in den Master Boot Record (MBR) der ersten Festplatte zu installieren, führen Sie den folgenden Befehl aus:

    ```
    setup (hd0)
    ```

11. Benden Sie die Shell von GRUB:

    ```
    quit
    ```

12. Trennen Sie die gemounteten Datei-Systeme und starten Sie dann neu:

    ```
    umount /mnt/system/dev/
    umount /mnt/system/proc/
    umount /mnt/system/boot/
    umount /mnt/system/
    reboot
    ```

13. Rekonfigurieren Sie den Boot-Loader durch die Verwendung von Tools und der Dokumentation, die zur von Ihnen verwendeten Linux-Distribution gehört. In Debian und Ubuntu z.B. müssen Sie vermutlich einige kommentierte Zeilen in der Datei **/boot/grub/menu.lst** bearbeiten und dann das Script **update-grub** ausführen; ansonsten treten die Änderungen nicht in Kraft.

5.5.2 Über Windows-Loader

Windows NT/2000/XP/2003

Ein Teil der Loader ist im Boot-Sektor hinterlegt, der Rest befindet sich in den Dateien ntldr, boot.ini, ntdetect.com, ntbootdd.sys. Boot.ini ist eine Textdatei, die die Konfiguration des Loaders enthält. Beispiel:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista und später

Ein Teil des Loaders ist im Boot-Sektor hinterlegt, der Rest in den Dateien bootmgr und boot\bcd. Während des Windows-Starts wird boot\bcd in den Registry-Schlüssel HKLM \BCD00000000 gemountet.

5.6 Ein Windows-System auf Werkseinstellungen zurücksetzen

Falls Ihr Windows-Betriebssystem unter Verwendung von Acronis Backup für System Builders bereitgestellt wurde, dann können Sie das System auf seine Werkseinstellungen zurücksetzen.

Das Zurücksetzen des Systems auf seine Werkseinstellungen kann von der Management Konsole oder beim Booten gestartet werden. Die zweite Methode ist nützlich, wenn das Betriebssystem aus irgendeinem Grund seine Bootfähigkeit verloren hat.

- Klicken Sie, um die Aktion von der Management Konsole aus zu starten, auf den Befehl **Auf Werkseinstellungen zurücksetzen** (in der **Willkommensseite**).
- Drücken Sie, um die Aktion beim Booten zu starten, einen 'Hot Key' (üblicherweise F11) und klicken Sie in der erscheinenden Anzeige dann auf **Auf Werkseinstellungen zurücksetzen**. Alternativ können Sie auch mit dem Booten des Betriebssystems fortfahren.

Sobald Sie die Aktion bestätigen, wird Acronis Backup das Image der Werkskonfiguration (Factory Image), welches in der Acronis Secure Zone gespeichert ist, erneut bereitstellen. Dadurch werden das ursprüngliche Volume-Layout, das vorinstallierte Windows-Betriebssystem und mögliche ursprüngliche Dritthersteller-Anwendungen wiederhergestellt, Die Software entfernt zusätzlich alle Benutzer-Archive aus der Acronis Secure Zone und setzt die Acronis Secure Zone wieder auf ihre ursprüngliche Größe zurück.

***Vorsicht:** Alle auf den ursprünglichen Laufwerken der Maschine gespeicherten Benutzerdaten gehen verloren.*

Manchmal kann ein System nicht auf die Werkseinstellungen zurückgesetzt werden, auch nicht beim Booten. Das kann beispielsweise der Fall sein, wenn es zu einem Laufwerksfehler kommt, falls das Factory Image in der Acronis Secure Zone beschädigt wurde oder das ursprüngliche Laufwerk durch ein neues ersetzt wurde. In diesem Fall können Sie das System dennoch auf die Werkseinstellungen zurücksetzen – und zwar, indem Sie das 'Bootfähige Medium mit Werkseinstellungen' (Factory Bootable Media) verwenden, sofern es mit Ihrer Maschine ausgeliefert wurde.

Booten Sie, um die Aktion zu starten, die Maschine mit diesem 'Factory Bootable Media' und klicken Sie in der erscheinenden Anzeige auf **Auf Werkseinstellungen zurücksetzen**. Sobald Sie die Aktion bestätigen, wird Acronis Backup eine Acronis Secure Zone erstellen und das Factory Image dorthin kopieren. Danach wird es das Factory Image, so wie weiter oben beschrieben, erneut bereitstellen.

Weitere Informationen finden Sie unter 'Acronis Secure Zone (S. 166)' und 'Acronis Startup Recovery Manager (S. 202)'.

5.7 Standardoptionen für Recovery

Jeder Acronis Agent hat eigene Standardoptionen für Recovery. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Recovery-Tasks können Sie entweder eine Standardoption verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Task gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Recovery-Tasks verwendet.

Um die Standardoptionen für Recovery einsehen und verändern zu können, verbinden Sie die Konsole mit der verwalteten Maschine und wählen Sie dort aus dem Hauptmenü die Befehle **Optionen –> Standardoptionen für Backup und Recovery –> Standardoptionen für Recovery**.

Verfügbarkeit der Recovery-Optionen

Art und Umfang der verfügbaren Recovery-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent arbeitet (Linux, bootfähige Medien).
- Dem Datentyp, der gesichert wird (Laufwerke, Dateien).
- Das Betriebssystem, das aus dem Disk-Backup wiederhergestellt wird

Die nachfolgende Tabelle fasst die Verfügbarkeit der Recovery-Optionen zusammen:

	Agent für Windows		**Bootfähiges Medium (Linux-basiert oder PE-basiert)**	
	Laufwerk-Recovery	**Datei-Recovery (auch aus Laufwerk-Backup)**	**Laufwerk -Recovery**	**Datei-Recovery (auch aus Laufwerk-Backup)**
Erweiterte Einstellungen (S. 143):				
Backup-Archiv vor der Wiederherstellung validieren	+	+	+	+
Maschine automatisch neu starten, wenn dies zur Wiederherstellung erforderlich ist	+	+	-	-
Nach Abschluss der Wiederherstellung die Maschine automatisch neu starten	-	-	+	+
Dateisystem nach Wiederherstellung prüfen	+	-	+	-
SID nach Wiederherstellung ändern	Windows-Recovery	-	Windows-Recovery	-
Aktuelles Datum und Zeit für wiederhergestellte Dateien festlegen	-	+	-	+
E-Mail-Benachrichtigungen (S. 144)	+	+	-	-
Fehlerbehandlung (S. 145):				
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)	+	+	+	+
Bei Fehler erneut versuchen	+	+	+	+
Ereignisverfolgung:				
Ereignisanzeige von Windows (S. 147)	+	+	-	-

	Agent für Windows		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Recovery	Datei-Recovery (auch aus Laufwerk-Backup)	Laufwerk -Recovery	Datei-Recovery (auch aus Laufwerk-Backup)
SNMP (S. 146)	+	+	-	-
Sicherheit auf Dateiebene (S. 147):				
Dateien mit ihren Sicherheitseinstellungen wiederherstellen	-	+	-	+
Mount-Punkte (S. 147)	-	+	-	-
Vor-/Nach-Befehle für Wiederherstellung (S. 148)	+	+	nur PE	nur PE
Recovery-Priorität (S. 149)	+	+	-	-

5.7.1 Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Recovery durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Aktuelles Datum und Zeit für wiederhergestellte Dateien festlegen

Diese Option ist nur wirksam, wenn Dateien wiederhergestellt werden.

Voreinstellung ist: **Aktiviert**.

Diese Option definiert, ob der Zeitstempel der wiederhergestellten Dateien aus dem Archiv übernommen wird oder ob den Dateien das aktuelle Datum und die aktuelle Zeit zugewiesen werden.

Backups vor Wiederherstellung validieren

Voreinstellung ist: **Deaktiviert**.

Diese Option definiert, ob ein Backup vor der Wiederherstellung der darin enthaltenen Daten zu validieren ist, um sicherzustellen, dass das Backup nicht beschädigt ist.

Dateisystem nach Wiederherstellung prüfen

Diese Option ist nur wirksam, wenn Laufwerke oder Volumes wiederhergestellt werden.

Voreinstellung ist: **Deaktiviert**.

Diese Option definiert, ob nach der Wiederherstellung eines Laufwerks oder Volumes die Integrität des wiederhergestellten Dateisystems geprüft wird. Die Überprüfung wird entweder direkt nach der Wiederherstellung ausgeführt oder nachdem die Maschine mit dem wiederhergestellten Betriebssystem gebootet hat.

Maschine automatisch neu starten, wenn dies zur Wiederherstellung erforderlich ist

Diese Option ist wirksam, wenn die Wiederherstellung auf einer Maschine mit laufendem Betriebssystem erfolgt.

Voreinstellung ist: **Deaktiviert**.

Die Option definiert, ob die Maschine automatisch neu gestartet wird, wenn das für die Wiederherstellung erforderlich ist. Dies ist beispielsweise der Fall, wenn ein Volume wiederhergestellt werden muss, welches vom Betriebssystem gesperrt wird.

Nach Abschluss der Wiederherstellung die Maschine automatisch neu starten

Diese Option ist wirksam, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Voreinstellung ist: **Deaktiviert**.

Diese Option ermöglicht den Neustart der Maschine in das wiederhergestellte Betriebssystem ohne weitere Aktion eines Benutzers.

5.7.2 E-Mail-Benachrichtigungen

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen über den erfolgreichen Abschluss von Recovery-Tasks, über Fehler oder wenn ein Benutzereingriff erforderlich ist.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung senden**, um die entsprechende Funktion zu aktivieren.
2. Aktivieren Sie unter **E-Mail-Benachrichtigungen schicken** die entsprechenden Kontrollkästchen folgendermaßen:
   - **Wenn die Wiederherstellung erfolgreich abgeschlossen wurde**.
   - **Wenn die Wiederherstellung fehlschlägt**.
   - **Wenn Benutzereingriff erforderlich ist**.
3. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
4. Geben Sie im Feld **Betreff** eine Beschreibung für die Benachrichtigung ein.

   Die Betreffzeile kann gewöhnlichen Text und eine oder mehrere Variablen enthalten. In den empfangenen E-Mail-Nachrichten wird jede Variable dann durch den zum Zeitpunkt der Task-Ausführung vorliegenden Wert ersetzt. Folgende Variablen werden unterstützt:
   - **%description%**

     Bei einer unter Windows laufenden Maschine wird die Variable **%description%** durch einen Text ersetzt, der dem Feld **Computerbeschreibung** der jeweiligen Maschine entspricht. Um den Text spezifizieren zu können, können Sie entweder zu **Systemsteuerung –> System** gehen oder folgenden Befehl als Administrator ausführen:

     ```
     net config server /srvcomment:<text>
     ```


Bei einer unter Linux laufenden Maschine wird die Variable **%description%** durch einen leeren String ("") ersetzt.

- **%subject%**

  Die Variable **%subject%** wird in folgenden Ausdruck umgewandelt: *Task <Task-Name> <Task-Ergebnis> auf Maschine <Maschinenname>.*

5. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
6. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
7. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
8. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:

   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.

   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.

   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:

      - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
      - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
      - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.

   d. Klicken Sie auf **OK**.
9. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

5.7.3 Fehlerbehandlung

Diese Optionen sind für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler beim Recovery behandelt werden.

Während der Durchführung keine Meldungen bzw. Dialoge zeigen (stiller Modus)

Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die einen Benutzereingriff erfordern, falls das möglich ist. Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler erneut versuchen

Voreinstellung ist: **Aktiviert**. **Zahl der Versuche: 30. Abstand zwischen Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Wenn der Speicherort im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

5.7.4 Ereignisverfolgung

Es ist möglich, die von den Recovery-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

5.7.4.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Recovery-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup siehe „Unterstützung für SNMP (S. 34)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Maschinen-Optionen definiert sind.**

So wählen Sie, ob Ereignisse von Recovery-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen finden Sie bei Maschinen-Optionen.
- **SNMP-Benachrichtigungen über Ereignisse von Recovery-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Recovery-Aktionen an spezifizierte SNMP-Manager.
  - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
  - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
  - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist 'Public'.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.
- **Keine SNMP-Benachrichtigungen senden** – Einstellung, um das Versenden von Ereignissen über Recovery-Aktionen an SNMP-Manager unwirksam zu machen.

5.7.4.2 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Recovery-Aktionen in der Windows Ereignisanzeige (Unterpunkt Anwendungen) aufzeichnen müssen (um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**). Sie können die Ereignisse filtern, die geloggt werden.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

Wählen Sie, ob Ereigniseinträge der Recovery-Aktionen an die Ereignisanzeige von Windows übergeben werden.

Wählen Sie eine der nachfolgenden Varianten:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Recovery-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
  - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
  - **Fehler und Warnungen**
  - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Recovery-Aktionen in der Ereignisanzeige.

5.7.5 Sicherheit auf Dateiebene

Diese Option ist nur für Wiederherstellungen von Windows-Dateien auf Dateiebene wirksam.

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien wiederhergestellt werden.

Voreinstellung ist: **Dateien mit ihren Sicherheitseinstellungen wiederherstellen**.

Wenn die NTFS-Zugriffsrechte auf die Dateien während des Backups (S. 100) erhalten wurden, können Sie wählen, ob Sie die Zugriffsrechte wiederherstellen oder ob Sie die Erlaubnis erteilen, dass die Dateien die NTFS-Zugriffsrechte vom Ordner erben, in den sie wiederhergestellt werden.

5.7.6 Mount-Punkte

Diese Option ist nur unter Windows zur Wiederherstellung von Daten aus einem dateibasierten Backup wirksam.

Aktivieren Sie die Option **Mount-Punkte**, um Dateien und Ordner wiederherzustellen, die auf gemounteten Volumes gespeichert waren und mit aktivierter Option **Mount-Punkte** gesichert wurden. Weitere Details zum Backup von gemounteten Volumes oder freigegebenen Cluster-Volumes finden Sie unter Mount-Punkte (S. 101).

Voreinstellung ist: **Deaktiviert**.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. Wenn Sie einen Ordner innerhalb des Mount-Punktes oder den Mount-Punkt selbst für eine Recovery-Aktion wählen, werden die gewählten Elemente unabhängig vom Wert der Option '**Mount-Punkte**' wiederhergestellt.

Beachten Sie, dass für den Fall, dass das Volume zum Recovery-Zeitpunkt nicht gemountet ist, die Daten direkt zu demjenigen Ordner wiederhergestellt werden, der zum Backup-Zeitpunkt der Mount-Punkt war.

5.7.7 Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenwiederherstellung durchgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Starten Sie den Befehl **`Checkdisk`**, damit logische Fehler im Dateisystem, physikalische Fehler oder fehlerhafte Sektoren vor Beginn oder nach Ende der Recovery-Aktion gefunden und behoben werden.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Recovery ausführen**
   - **Nach Recovery ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

5.7.7.1 Befehl vor Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start der Wiederherstellung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	Auswahl			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Keine Wiederherstellung bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Recovery nur durchführen, nachdem der Befehl erfolgreich ausgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Recovery nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Recovery gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

5.7.7.2 Befehl nach Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn die Wiederherstellung vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** ein Kommando ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
3. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
4. Aktivieren Sie das Kontrollkästchen **Task scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Falls die Befehlsausführung fehlschlägt, wird das auch das Ergebnis der Task-Aktion auf 'fehlgeschlagen' gesetzt.

   Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Einsicht in die Anzeige **Log** verfolgen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

5.7.8 Recovery-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Grad der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Recovery-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der

Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Voreinstellung ist: **Normal.**

So spezifizieren Sie die Priorität des Recovery-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Recovery-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Recovery-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Recovery-Prozesses und zieht Ressourcen von anderen Prozessen ab.

6 Konvertierung zu einer virtuellen Maschine

Acronis Backup ermöglicht mehrere Möglichkeiten, ein Laufwerk-Backup in eine virtuelle Maschine zu konvertieren. Dieser Abschnitt soll Ihnen helfen, die Methode zu finden, die Ihren Bedürfnissen am besten entspricht – und stellt Schritt-für-Schritt-Anleitungen zur Konvertierung bereit.

6.1 Konvertierungsmethoden

Sie können, abhängig von Ihren Anforderungen, zwischen folgenden Konvertierungsmethoden wählen:

a) **Die Konvertierung zum Teil eines Backup-Plans machen**

Zeitpunkt der Verwendung.

- Falls Sie möchten, dass das Backup und die Konvertierung nach Planung ausgeführt werden. Das hilft Ihnen, einen auf Standby stehenden virtuellen Server aufrechtzuerhalten, falls Ihr physikalischer Server ausfällt.
- Falls Sie die resultierenden Einstellungen der virtuellen Maschine nicht anpassen müssen.

Art der Durchführung. Aktivieren Sie bei Erstellung eines Backup-Plans (S. 38) die Funktion zur Konvertierung eines Backups zu einer virtuellen Maschine (S. 153).

b) **Wiederherstellung der gesicherten Laufwerke oder Volumes mit dem Ziel 'Neue virtuelle Maschine'**

Zeitpunkt der Verwendung.

- Falls Sie die Konvertierung bei Bedarf einmalig oder gelegentlich durchführen wollen.
- Falls Sie eine verlustfreie Migration von 'Physikalisch zu virtuell' durchführen wollen. Booten Sie in diesem Fall die ursprüngliche Maschine mit einem bootfähigen Medium, erstellen Sie ein Backup der Maschine im Offline-Stadium und stellen Sie die Maschine dann direkt aus dem resultierenden Backup wieder her.
- Falls Sie die resultierenden Einstellungen der virtuellen Maschine anpassen müssen. Sie können Laufwerke hinzufügen oder entfernen, den Provisioning-Modus für Laufwerke wählen, die Größe und den Speicherort von Volumes auf den Laufwerken ändern und mehr.

Art der Durchführung. Folgen Sie den im Abschnitt 'Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 157)' beschriebenen Schritten.

c) **Wiederherstellung der gesicherten Laufwerke oder Volumes unter Verwendung eines bootfähigen Mediums zu einer manuell erstellten virtuellen Maschine**

Zeitpunkt der Verwendung.

- Falls Sie eine Maschine direkt auf einem Virtualisierungsserver erstellen wollen, statt sie zu importieren.

  Tipp: Mit dem Agenten für VMware oder dem Agenten für Hyper-V kann eine virtuelle Maschine direkt auf einem entsprechenden Virtualisierungsserver mit den Methoden (a) und (b) erstellt werden.
- Falls Sie dynamische Volumes auf einer Windows-Maschine neu erstellen müssen.
- Falls Sie logische Volumes oder ein Software-RAID auf einer Linux-Maschine neu erstellen müssen.

Art der Durchführung. Folgen Sie den im Abschnitt 'Wiederherstellung zu einer manuell erstellten virtuellen Maschine (S. 160)' beschriebenen Schritten.

6.2 Konvertierung zu einer automatisch erstellten virtuellen Maschine

Dieser Abschnitt beschreibt die Konvertierungsmethoden (S. 151), mit denen Acronis Backup eine neue virtuelle Maschine automatisch erstellt:

- Während einer Konvertierung, die Teil eines Backup-Plans ist (S. 153), erstellt die Software die virtuelle Maschine zusätzlich zur Erstellung des Backups. Die virtuelle Maschine hat dieselbe Konfiguration wie die ursprüngliche Maschine.
- Während einer Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 157) erstellt die Software die virtuelle Maschine von einem Backup, welches bereits vorliegt. Sie können die Konfiguration der virtuellen Maschine ändern.

Acronis Backup kann, abhängig von dem die Konvertierung durchführenden Agenten, eine virtuelle Maschine mit jedem der folgenden Formate erstellen:

Agent für Windows, Agent für Linux

- VMware Workstation
- Microsoft Virtual PC (einschließlich Windows Virtual PC)
- Citrix XenServer OVA (nur während einer Wiederherstellung zum Ziel 'Neue virtuelle Maschine')
- Kernel-based Virtual Machine
- Red Hat Enterprise Virtualization (RAW-Format)

Agent für VMware

- VMware ESX(i)

Agent für Hyper-V

- Microsoft Hyper-V

6.2.1 Überlegungen vor der Konvertierung

Konvertieren einer UEFI-basierten Maschine

Virtuellen Maschinen, die UEFI (Unified Extensible Firmware Interface) verwenden, werden derzeit nur in VMware ESXi 5 unterstützt. Falls es sich bei der als Ziel dienenden Virtualisierungsplattform um ESXi 5 handeln, dann erstellt Acronis Backup eine UEFI-basierte Maschine. Anderenfalls wird die resultierende Maschine die BIOS-Boot-Firmware verwenden.

Acronis Backup passt den Windows-Boot-Modus an die BIOS-Boot-Firmware an und stellt so sicher, dass Windows bootfähig bleibt.

Bei Linux-Betriebssystemen wird eine Änderung des Boot-Modus von UEFI zu BIOS nicht unterstützt. Stellen Sie bei Konvertierung einer unter Linux laufenden, UEFI-basierten Maschine sicher, dass diese GRUB Version 1 verwendet und dass die Zielvirtualisierungsplattform ESXi 5 ist. Weitere Details finden Sie im Abschnitt 'Unterstützung für UEFI-basierte Maschinen (S. 36)'.

Logische und dynamische Volumes

Die resultierende Maschine wird Basis-Volumes haben, selbst wenn im Backup eine logische Linux-Volume-Struktur vorliegt. Dasselbe gilt für dynamische, unter Windows verwendete Volumes. Falls Sie auf der Maschine logische oder dynamische Volumes neu erstellen wollen, dann führen Sie die Konvertierung so durch, wie im Abschnitt 'Wiederherstellung zu einer manuell erstellten virtuellen Maschine (S. 160)' beschrieben.

Reaktivierung eines benutzerdefinierten Loaders (Custom Loader)

- Die Laufwerksschnittstellen können während der Konvertierung geändert werden, etwa als Ergebnis der Migration zu einer anderen Plattform oder wegen manueller Anpassung. Die Software stellt die Systemlaufwerkschnittstelle so ein, dass sie der Standardschnittstelle der neuen Plattform entspricht. Für VMWare ist die Standardschnittstelle SCSI, für andere unterstützte Plattformen ist sie IDE. Wenn sich die Schnittstelle des Systemlaufwerks ändert, dann ändert sich auch der Name des Boot-Gerätes; der Bootloader verwendet jedoch weiterhin den alten Namen.
- Eine Konvertierung von logischen Volumes zu solchen vom Typ 'Basis' kann außerdem bewirken, dass das System nicht mehr booten kann.

Falls die Maschine einen benutzerdefinierten Boot-Loader (Custom Loader) verwendet, müssen Sie diesen daher evtl. so konfigurieren, dass er auf die neuen Geräte verweist und den Loader reaktivieren. Eine Konfiguration von GRUB ist normalerweise nicht notwendig, weil Acronis Backup dies automatisch durchführt. Sollte es doch notwendig sein, dann verwenden Sie die im Abschnitt 'So reaktivieren Sie GRUB und ändern seine Konfiguration (S. 139)' beschriebene Prozedur.

Weitere Überlegungen zur Konvertierung von physikalischen zu virtuellen Maschinen finden Sie im Dokument 'Backups von virtuellen Maschinen'.

6.2.2 Regelmäßige Konvertierung zu einer virtuellen Maschine einrichten

Sie können bei Erstellung eines Backup-Plans (S. 38) einstellen, dass Laufwerk- oder Volume-Backups regelmäßig zu einer virtuellen Maschine konvertiert werden. Durch Einrichten einer regelmäßigen Konvertierung erhalten Sie eine Kopie Ihres Servers oder Ihrer Workstation in Form einer virtuellen Maschine, die sofort einsatzbereit ist, falls die ursprüngliche Maschine ausfallen sollte.

Einschränkungen

- Eine Backup-Konvertierung ist von folgenden Speicherorten aus nicht verfügbar: CDs, DVDs, Blu-Ray-Discs, Bandgeräte und der Acronis Cloud Storage.
- Die Konvertierung zu einer virtuellen Maschine vom Typ 'Citrix XenServer' ist als Bestandteil eines Backup-Plans nicht verfügbar. Verwenden Sie als Alternative die Methoden (b) und (c), wie im Abschnitt 'Konvertierungsmethoden (S. 151)' beschrieben.
- Microsoft Virtual PC unterstützt keine virtuellen Laufwerke, die größer als 127 GB sind. Während der Konvertierung zu einer Virtual PC-Maschine wird die Größe eines jeden Laufwerks, welches 127 GB überschreitet, auf diesen Wert verkleinert. Sollte die Größenanpassung des Laufwerks nicht möglich sein, schlägt die Konvertierung fehl. Sollten Sie größere virtuelle Laufwerke benötigen, um diese an eine Hyper-V-Maschine anzubinden, dann verwenden Sie die unter 'Konvertierungsmethoden (S. 151)' beschriebenen Methoden (b) und (c).

6.2.2.1 Konvertierungseinstellungen

Die Informationen in diesem Abschnitt sollen Ihnen helfen, die passenden Konvertierungseinstellungen vorzunehmen.

Die Einstellungen werden im Bereich **Zu virtueller Maschine konvertieren** der Seite **Backup-Plan erstellen** spezifiziert.

Zu virtueller Maschine konvertieren

Konvertierungsquelle

Falls Sie Backups zu anderen Speicherorten kopieren oder verschieben (S. 79), dann wählen Sie den Speicherort, von dem das Backup genommen werden soll.
Konvertierungsspeicherorte, die nicht verfügbar (S. 153) sind (wie der Acronis Cloud Storage) werden nicht aufgelistet.

Standardmäßig werden Konvertierungen vom primären Speicherort aus durchgeführt.

Konvertierungszeitpunkt

Spezifizieren Sie, abhängig vom gewählten Backup-Schema, ob jedes vollständige, inkrementelle oder differentielle Backup konvertiert werden soll oder das jeweils letzte nach Planung erstellte Backup. Spezifizieren Sie bei Bedarf die **Konvertierungsplanung** (S. 154).

Ziel-Host... (S. 155)

Bestimmen Sie den Typ und Speicherort der resultierenden virtuellen Maschine. Die verfügbaren Optionen hängen von dem Agenten ab, der die Konvertierung durchführt. Das kann der Agent sein, der (standardmäßig) das Backup durchführt oder ein Agent, der auf einer anderen Maschine installiert ist. Im letzteren Fall muss das Archiv an einem gemeinsam nutzbaren Ort gespeichert werden, z.B. einem Netzwerkordner oder einem verwalteten Depot, damit die andere Maschine auf das Archiv zugreifen kann.

Klicken Sie zur Spezifikation eines anderen Agenten auf **Ändern** und wählen Sie eine Maschine, auf der ein Agent für VMware, ein Agent für Hyper-V, ein Agent für Windows oder ein Agent für Linux installiert ist.

Storage

Wählen Sie den Storage auf dem Virtualisierungsserver oder den Ordner, wo die Dateien der virtuellen Maschine gespeichert werden sollen.

Resultierende VMs

Spezifizieren Sie den Namen der virtuellen Maschine. Die vorgegebene Bezeichnung ist **Backup_von_[Maschinenname]**. Sie können dem Namen weitere Variablen hinzufügen. Folgende Vorlagen werden unterstützt:

[Plan-Name]
[Maschinenname]
[Virtueller Host-Name]
[Name der virtuellen Maschine]
[Virtualisierungsservertyp]

Ordner auf dem VMware vCenter

Wenn der Management Server mit dem vCenter Server integriert ist, erscheinen die resultierenden Maschinen im Ordner **Acronis Backups** auf dem vCenter. Sie können einen Unterordner für die Maschinen spezifizieren, die aus der Ausführung des Plans resultieren.

6.2.2.2 Eine Konvertierungsplanung einrichten

Ein bei Ausführung eines Backup-Plans erstelltes Laufwerk-Backup (S. 299) kann sofort oder per Planung zu einer virtuellen Maschine konvertiert werden – oder durch eine Kombination beider Methoden.

Der Konvertierungstask wird auf der zu sichernden Maschine erstellt und verwendet die Zeiteinstellungen der Maschine. Falls der Agent, der die Maschine sichert, außerhalb von dieser installiert ist (ist der Fall, wenn virtuelle ESX(i)- oder Hyper-V-Maschinen auf Hypervisor-Ebene gesichert werden), dann wird der Task auf der Maschine erstellt, auf der sich der Agent befindet.

Die virtuelle Zielmaschine muss zum Zeitpunkt der Konvertierung heruntergefahren sein, sonst schlägt der Konvertierungstask fehl. Sollte das passieren, dann können Sie den Konvertierungstask

manuell neu starten, nachdem die betreffende Maschine ausgeschaltet wurde. Änderungen, die an der Maschine durchgeführt wurden, während sie eingeschaltet war, werden überschrieben.

6.2.2.3 Eine Maschine zur Durchführung von Konvertierungen wählen

Berücksichtigen Sie folgende Überlegungen.

Welcher Agent ist auf der Maschine installiert?

Typ und Speicherort der resultierenden virtuellen Maschine hängen von dem Agenten ab, der auf der gewählten Maschine vorliegt.

- Der **Agent für VMware** ist auf der Maschine installiert

  Falls der Agent mehr als einen ESX(i)-Host verwaltet, dann können Sie den Host wählen, auf dem die virtuelle Maschine erstellt wird.

  Im Schritt **Storage** können Sie den Speicherort/-Typ wählen, wo die virtuelle Maschine erstellt wird.

  Als Ergebnis eines Backups erstellte virtuelle Maschinen können einem Backup-Plan nicht hinzugefügt werden. Sie erscheinen auf dem Management Server als 'nicht verwaltbar' oder erscheinen überhaupt nicht (falls keine Integration mit dem vCenter-Server aktiviert ist).
- Der **Agent für Hyper-V** ist auf der Maschine installiert

  Sie können eine virtuelle Maschine nur auf dem Hyper-V-Server erstellen.

  Im Schritt **Storage** können Sie den Pfad zur virtuellen Maschine wählen.

  Infolge eines Backups auf dem Server erstellte virtuelle Maschinen erscheinen nicht auf dem Management Server, weil solche Maschinen nicht dazu gedacht sind, per Backup gesichert zu werden.
- Der **Agent für Windows** oder der **Agent für Linux** sind auf der Maschine installiert

  Sie können den Typ der virtuellen Maschine wählen: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM) oder Red Hat Enterprise Virtualization (RHEV).

  Im Schritt **Storage** können Sie den Pfad zur virtuellen Maschine wählen.

Wie ist die Rechenleistung der Maschine?

Die Konvertierung belastet die CPU-Ressourcen der gewählten Maschine. Mehrere Konvertierungstasks werden auf dieser Maschine über eine Warteschlange abgearbeitet, deren vollständige Abarbeitung eine beträchtliche Zeit benötigen kann. Sie sollten dies berücksichtigen, wenn Sie einen zentralen Backup-Plan mit Konvertierung mehrerer Maschinen erstellen – oder wenn Sie mehrere lokale Backup-Pläne erstellen, die dieselbe Maschine zur Konvertierung verwenden.

Welcher Storage wird für die virtuellen Maschinen verwendet?

Netzwerkauslastung

Im Gegensatz zu üblichen Backups (tib-Dateien) werden die 'Virtuellen Maschinen'-Dateien unkomprimiert durch das Netzwerk übertragen. Aus Sicht der Netzwerkauslastung ist es daher am besten, ein SAN oder einen lokalen Storage für die Maschine zu verwenden, die die Konvertierung ausführt. Sie können jedoch kein lokales Laufwerk wählen, wenn die Konvertierung von derselben Maschine durchgeführt wird, die auch gesichert wird. Die Verwendung eines NAS macht ebenfalls Sinn.

Speicherplatz

Bei VMware, Hyper-V und Virtual PC werden die Laufwerke der resultierenden virtuellen Maschine so viel Speicherplatz wie die ursprünglichen Daten belegen. Bei einer angenommenen ursprünglichen Laufwerksgröße von 100 GB, von denen 10 GB mit Daten belegt sind, ergibt sich ein entsprechendes virtuelles Laufwerk von ebenfalls ca. 10 GB. VMware nennt dieses Format 'Thin Provisioning', Microsoft verwendet den Begriff 'Laufwerk mit dynamischer Erweiterung' (Dynamically Expanding Disk). Da der Speicherplatz nicht vorab zugeordnet wird, wird für den physikalischen Storage angenommen, dass er noch genügend freien Speicherplatz hat, damit die virtuellen Laufwerke auch noch an Größe zunehmen können.

Bei KVM oder RHEV werden die Laufwerke der resultierenden virtuellen Maschine das Raw-Format haben. Das bedeutet, dass die virtuelle Laufwerksgröße immer gleich zur ursprünglichen Laufwerkskapazität ist. Angenommen, die ursprüngliche Laufwerksgröße beträgt 100 GB, dann wird das korrespondierende virtuelle Laufwerk 100 GB belegen, selbst wenn das Laufwerk nur Daten von 10 GB speichert.

6.2.2.4 Wie die 'regelmäßige Konvertierung zu VM' arbeitet

Wie die wiederholte Konvertierung arbeitet, hängt davon ab, wo nach Ihrer Wahl die virtuelle Maschine erstellt werden soll.

- **Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll:** Erstellt jede Konvertierung die virtuelle Maschine von Grund aus neu.
- **Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll:** Aktualisiert die Software eine existierende virtuelle Maschine statt sie neu zu erstellen, wenn ein inkrementelles oder differentielles Backup konvertiert wird. Eine solche Konvertierung ist normalerweise schneller. Sie geht sparsamer mit Netzwerkverkehr und CPU-Ressourcen des Hosts um, der die Konvertierung durchführt. Falls eine virtuelle Maschine nicht aktualisiert werden kann, erstellt die Software auch diese von Grund auf neu.

Nachfolgend finden Sie eine genauere Beschreibung beider Fälle.

Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll

Als Folge der ersten Konvertierung wird eine neue virtuelle Maschine erstellt. Jede nachfolgende Konvertierung wird diese Maschine jeweils ganz neu erstellen. Zuerst wird die alte Maschine temporär umbenannt. Dann wird eine neue virtuelle Maschine erstellt, die den vorherigen Namen der alten Maschine hat. Sobald diese Aktion erfolgreich abgeschlossen wurde, wird die alte Maschine gelöscht. Wenn die Aktion fehlschlägt, wird die neue Maschine gelöscht und die alte Maschine erhält ihren früheren Namen zurück. Auf diese Art schließt die Konvertierung immer mit einer einzelnen Maschine ab. Jedoch wird während der Konvertierung zusätzlicher Speicherplatz benötigt, um die alte Maschine aufzunehmen.

Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll

Die erste Konvertierung erstellt eine ganz neue virtuelle Maschine. Jede nachfolgende Konvertierung arbeitet folgendermaßen:

- Falls es seit der letzten Konvertierung ein *Voll-Backup* gegeben hat, wird die virtuelle Maschine ganz neu erstellt (wie zuvor in diesem Abschnitt beschrieben).
- Anderenfalls wird die existierende virtuelle Maschine so aktualisiert, dass sie die Änderungen seit der letzten Konvertierung widerspiegelt. Wenn eine Aktualisierung (Update) nicht möglich ist

(beispielsweise, weil Sie die zwischenzeitlichen Snapshots gelöscht haben, siehe nachfolgend), wird die virtuelle Maschine ganz neu erstellt.

Zwischenzeitliche Snapshots

Um die virtuelle Maschine aktualisieren zu können, speichert die Software einige zwischenzeitliche Snapshots von ihr. Sie werden **Backup…** und **Replica…** genannt und sollten behalten werden. Nicht mehr benötigte Snapshots werden automatisch gelöscht.

Der jüngste **Replikat…**-Snapshot korrespondiert mit dem Ergebnis der letzten Konvertierung. Sie können zu diesem Snapshot zurückgehen, falls Sie die Maschine auf dieses Stadium zurücksetzen wollen – beispielsweise, weil Sie mit der Maschine gearbeitet haben und nun durchgeführte Änderungen verwerfen wollen.

Andere Snapshots sind nur zur internen Verwendung durch die Software.

6.2.3 Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine'

Statt eine tib-Datei einfach nur zu einer virtuellen Laufwerksdatei zu konvertieren (was zusätzliche Aktionen für die Verfügbarkeit des virtuellen Laufwerks erforderlich machen würde), führt Acronis Backup die Konvertierung so aus, dass das betreffende Laufwerk-Backup in Form einer neuen, vollständig konfigurierten und betriebsbereiten virtuellen Maschine wiederhergestellt wird. Sie können bei der Vorbereitung der Recovery-Aktion die Konfiguration der virtuellen Maschine an Ihre speziellen Anforderungen anpassen.

Sie können mit dem **Acronis Backup Agenten für Windows** oder dem **Agenten für Linux** eine neue virtuelle Maschine in einem lokalen Ordner oder Netzwerkordner erstellen. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine zukünftige Verwendung vorbereiten. Die folgende Tabelle fasst die verfügbaren virtuellen Maschinen-Formate und möglichen Aktionen zusammen, um die Maschine einem Virtualisierungsserver hinzuzufügen.

VM-Format	Weitere Aktion und zu verwendendes Tool	Zielvirtualisierungsplattform
VMware Workstation	Exportieren mit VMware Workstation; oder Konvertieren zu OVF mit dem VMware OVF-Toool > Deployment des OVF-Vorlagen mit dem vSphere Client	ESX(i)
Microsoft Virtual PC*	Die VHD-Datei einer Hyper-V-Maschine hinzufügen	Hyper-V
Citrix XenServer OVA	Importieren mit dem Citrix XenCenter	XenServer
Kernel-based Virtual Machine (Raw-Format)	Verschieben der virtuellen Maschinen-Dateien zu einer unter Linux laufenden Maschine und Ausführung der virtuellen Maschine mit dem Virtual Machine Manager	-
Red Hat Enterprise Virtualization (RHEV) (Raw-Format)	Importieren mit dem RHEV-Manager	RHEV

*Microsoft Virtual PC unterstützt keine Laufwerke, die größer als 127 GB sind. Acronis ermöglicht Ihnen, eine Virtual PC-Maschine mit größeren Laufwerken zu erstellen, so dass Sie die Laufwerke an eine virtuelle Microsoft Hyper-V-Maschine anbinden können.

Sie können mit dem **Acronis Backup Agenten für Hyper-V** oder **Agenten für VMware** eine neue virtuelle Maschine direkt auf dem entsprechenden Virtualisierungsserver erstellen.

6.2.3.1 Auszuführende Schritte

So führen Sie eine Wiederherstellung zu einer neuen virtuellen Maschine durch

1. Verbinden Sie die Konsole mit dem Management Server, mit einer Maschine, auf der ein Agent installiert ist oder mit einer Maschine, die mit einem bootfähigen Medium gestartet wurde.
2. Klicken Sie auf **Recovery**, um die Seite **Daten wiederherstellen** (S. 112) zu öffnen.
3. Klicken Sie auf **Daten wählen** (S. 114). Verwenden Sie die Registerlasche **Datenanzeige** oder **Archiv-Anzeige**, um die Laufwerke bzw. Volumes für die Konvertierung auszuwählen.
4. Wählen Sie unter **Recovery nach** das Element **Neue virtuelle Maschine**.
5. Klicken Sie auf **Durchsuchen**. Wählen Sie im Fenster **VM/VS-Auswahl** (S. 158) den resultierenden Typ der virtuellen Maschine oder den Virtualisierungsserver, auf dem die Maschine erstellt werden soll.
6. [Optional] Sie können bei **Storage** sehen oder wählen, wo die virtuelle Maschine erstellt wird.
7. [Optional] Sie können bei **Einstellungen der virtuellen Maschine** (S. 159) den Namen der neuen virtuellen Maschine, den 'Provisioning'-Laufwerksmodus, die Speicherzuteilung sowie andere Einstellungen ändern.

   Maschinen, die denselben Typ und denselben Namen haben, können nicht im selben Ordner erstellt werden. Wenn Sie eine Fehlermeldung erhalten, die durch identische Namen hervorgerufen wurde, dann ändern Sie entweder den VM-Namen oder den Pfad.

8. Das Ziellaufwerk für jedes der Quelllaufwerke bzw. Quell-Volumes und MBRs wird automatisch ausgewählt. Sie können die Ziellaufwerke bei Bedarf ändern.

   Unter Microsoft Virtual PC, wo sich der Loader des Betriebssystems auf Laufwerk 1 befindet, müssen Sie unbedingt dieses Laufwerk oder Volume wiederherstellen. Anderenfalls wird das Betriebssystem nicht booten. Das kann durch Ändern der Reihenfolge der Boot-Geräte im BIOS nicht repariert werden, weil Virtual PC diese Einstellungen ignoriert.

9. Geben Sie unter **Recovery-Zeitpunkt** an, wann der Recovery-Task beginnen soll.
10. [Optional] Überprüfen Sie bei **Task** die **Recovery-Optionen** und ändern Sie die Standardeinstellungen gegebenenfalls ab. Sie können bei **Recovery-Optionen –> VM-Energieverwaltung** spezifizieren, ob die neue virtuelle Maschine automatisch gestartet werden soll, nachdem die Wiederherstellung abgeschlossen wurde. Diese Option ist nur verfügbar, wenn die neue Maschine auf einem Virtualisierungsserver erstellt wird.
11. Klicken Sie auf **OK**. Wenn der Recovery-Task für einen späteren Zeitpunkt geplant ist, geben Sie die Anmeldedaten an, unter denen der Task ausgeführt wird.

Sie können in der Ansicht **Backup-Pläne und Tasks** das Stadium und den Fortschritt des Recovery-Tasks überprüfen.

6.2.3.2 Typ der virtuellen Maschine / Wahl des Virtualisierungsservers

Wählen Sie den resultierenden Typ der virtuellen Maschine oder den Virtualisierungsserver, auf dem die Maschine erstellt wird.

Die verfügbaren Optionen hängen von dem (den) Agent(en) ab, der (die) auf der Maschine installiert ist (sind), mit der die Konsole verbunden ist. Wenn die Konsole mit dem Management Server verbunden ist, können Sie jede registrierte Maschine wählen, die in der Lage ist, die erforderliche Aktion durchzuführen.

So bestimmen Sie den Virtualisierungsserver, auf dem die virtuelle Maschine erstellt wird

1. Wählen Sie die Option **Eine neue virtuelle Maschine auf dem Server erstellen**.

2. Wählen Sie im linken Teil des Fensters den Virtualisierungsserver. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Server einzusehen.

   [Nur, wenn die Konsole mit dem Management Server verbunden ist] Falls mehrere Agenten den ausgewählten ESX(i)-Host verwalten, können Sie den Agenten auswählen, der die Wiederherstellung durchführen soll. Wählen Sie zur Erreichung einer besseren Performance einen Agenten für VMware (Virtuelle Appliance), der sich auf dem ESX(i) befindet. Falls kein Agent den ESX(i) verwaltet und die Funktion Automatisches Deployment aktiviert ist, dann wird der Agent für VMware (Virtuelle Appliance) sofort bereitgestellt, nachdem Sie auf **OK** geklickt haben. Die Wiederherstellung wird von diesem Agenten durchgeführt. Er wird eine Lizenz in Anspruch nehmen.
3. Klicken Sie auf **OK**, um zur Seite **Daten wiederherstellen** zurückzukehren.

So wählen Sie den Typ der virtuellen Maschine

1. Wählen Sie die Option **Die virtuelle Maschine als eine Zusammenstellung von Dateien speichern**.
2. Wählen Sie im linken Teil des Fensters den Typ der virtuellen Maschine. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Typ der virtuellen Maschine einzusehen.

   [Nur, wenn die Konsole mit dem Management Server verbunden ist] Sie können die Maschine wählen, die die Wiederherstellung durchführen wird. Das kann jede registrierte Maschine sein, auf welcher der Agent für Windows oder der Agent für Linux installiert ist.
3. Klicken Sie auf **OK**, um zur Seite **Daten wiederherstellen** zurückzukehren.

6.2.3.3 Einstellungen der virtuellen Maschine

Sie können die nachfolgenden Einstellungen der virtuellen Maschinen konfigurieren.

Laufwerke

Anfangseinstellung: Die Zahl und Größe der Laufwerke der Quellmaschine.

Die Anzahl der Laufwerke ist üblicherweise gleich zu denen der Quellmaschine. Sie kann jedoch abweichen, wenn die Software weitere Laufwerke hinzufügen muss, um die Volumes der Quellmaschine aufzunehmen, weil das Virtualisierungsprodukt hier Limitierungen setzt. Sie können der Maschinen-Konfiguration weitere virtuelle Laufwerke hinzufügen oder in manchen Fällen das vorgeschlagene Laufwerk löschen.

Sie können beim Hinzufügen eines neuen virtuellen Laufwerkes zusammen mit seiner Schnittstelle und Kapazität auch das Format spezifizieren.

- **Format 'Thin' (Schlank).** Das Laufwerk belegt so viel Speicherplatz, wie es der Größe der gespeicherten Daten entspricht. Dadurch wird Speicherplatz gespart. Aktivieren Sie zur Nutzung dieses Formates das Kontrollkästchen **Thin Provisioning** (für ESX) oder **Laufwerk mit dynamischer Erweiterung** (für Hyper-V).
- **Format 'Thick'.** Das Laufwerk belegt den gesamten bereitgestellten Speicherplatz. Dies verbessert die Performance der virtuellen Maschine. Deaktivieren Sie zur Nutzung des Formates 'Thick' das Kontrollkästchen **Thin Provisioning** (für ESX) oder **Laufwerk mit dynamischer Erweiterung** (für Hyper-V).

Wenn eine physikalische Maschine gesichert wurde, ist die Standardeinstellung das Format 'Thick'. Bei Wiederherstellung des Backups einer virtuellen Maschine versucht die Software, das Laufwerksformat der ursprünglichen Maschine zu reproduzieren. Falls dies nicht möglich ist, wird das Format 'Thick' verwendet.

Die Implementierung von Xen-Maschinen basiert auf Microsoft Virtual PC und hat daher dieselben Einschränkungen: bis zu 3 IDE-Laufwerke und 1 Prozessor. SCSI-Laufwerke werden nicht unterstützt.

Arbeitsspeicher

Anfangseinstellung: Es ist die Standardeinstellung des Virtualisierungsservers, sofern nicht im Backup enthalten.

Dies ist die Menge des Hauptspeichers, der der neuen virtuellen Maschine zugeteilt wird. Der einstellbare Bereich für die Speicherzuteilung hängt von der Hardware des Hosts ab, dessen Betriebssystem und den Einstellungen des Virtualisierungsprodukts. Sie können beispielsweise festlegen, dass die virtuellen Maschinen nicht mehr als 30% des Arbeitsspeichers verwenden dürfen.

Name

Anfangseinstellung: falls nicht im Backup enthalten, **Neue virtuelle Maschine**.

Geben Sie den Namen für die neue virtuelle Maschine ein. Wurde das Backup durch den Agenten für VMware oder den Agenten für Hyper-V erstellt, dann übernimmt die Software den Namen aus der im Backup enthaltenen virtuellen Maschinen-Konfiguration.

Prozessoren

Anfangseinstellung: Es ist die Standardeinstellung des Servers, sofern nicht im Backup enthalten, oder falls die gesicherten Einstellungen vom Virtualisierungsserver nicht unterstützt werden.

Es handelt sich um die Zahl der Prozessoren für die neue virtuelle Maschine. In den meisten Fällen ist sie auf einen Prozessor eingestellt. Wird der Maschine mehr als ein Prozessor zugewiesen, so kann das Ergebnis nicht garantiert werden. Die Zahl virtueller Prozessoren kann durch die CPU-Konfiguration des Hosts, das Virtualisierungsprodukt und das Betriebssystems des Gastes limitiert werden. Üblicherweise stehen mehrere virtuelle Prozessoren auf Hosts zur Verfügung, die selbst mehrere Prozessoren haben. Eine Multi-Core-Host-CPU oder Hyper-Threading kann mehrfache virtuelle Prozessoren auch auf einem Single-Prozessor-Host ermöglichen.

6.3 Wiederherstellung zu einer manuell erstellten virtuellen Maschine

Dieser Abschnitt beschreibt die Konvertierungsmethode (S. 151), bei der Sie selbst eine virtuelle Maschine erstellen und eine Wiederherstellung zu ihr so durchführen, als ob es sich um eine physikalische Maschine handelt.

6.3.1 Überlegungen vor der Konvertierung

Konvertieren einer UEFI-basierten Maschine

Sollte die ursprüngliche Maschine UEFI (Unified Extensible Firmware Interface) zum Booten verwenden, dann sollten Sie erwägen, eine virtuelle Maschine zu erstellen, die ebenfalls UEFI-basiert ist.

Sollte Ihr Virtualisierungsprodukt kein UEFI unterstützen, dann können Sie eine BIOS-basierte Maschine erstellen, sofern die ursprüngliche Maschine unter Windows lief. Acronis Backup passt den Windows-Boot-Modus an die BIOS-Boot-Firmware an und stellt so sicher, dass Windows bootfähig bleibt.

Bei Linux-Betriebssystemen wird eine Änderung des Boot-Modus von UEFI zu BIOS nicht unterstützt. Acronis Backup kann eine unter Linux laufende, UEFI-basierte Maschine nur dann konvertieren, wenn die Maschine GRUB in Version 1 verwendet und die Zielmaschine ebenfalls UEFI-basiert ist. Weitere Details finden Sie unter 'Unterstützung für UEFI-basierte Maschinen (S. 36)'.

Wahl der Laufwerksschnittstelle

Möglicherweise möchten Sie beim Erstellen der virtuellen Maschine, dass deren Laufwerke eine andere Schnittstelle verwenden als die in der ursprünglichen Maschine.

- Sie möchten beispielsweise alle Laufwerksschnittstellen von IDE zu SCSI ändern, wenn Sie eine Maschine zu ESX(i) migrieren, weil SCSI die Standardlaufwerksschnittstelle bei ESX(i) ist und eine bessere Performance bietet.
- Sie müssen die Laufwerksschnittstelle des Systems von SCSI zu IDE ändern, wenn Sie eine Maschine zu Hyper-V migrieren, weil Hyper-V das Booten von SCSI-Laufwerken nicht unterstützt.

Falls die ursprüngliche Maschine einen selbsterstellten Boot-Loader verwendet, dann stellen Sie das Systemlaufwerk zu einem Laufwerk mit derselben Schnittstelle wieder her – oder konfigurieren Sie den Bootloader manuell. Hintergrund ist, dass bei Änderung der Schnittstelle des Systemlaufwerks sich auch der Name des Boot-Gerätes ändert; der Bootloader verwendet jedoch weiterhin den alten Namen. Eine Konfiguration von GRUB ist normalerweise nicht notwendig, weil Acronis Backup dies automatisch durchführt.

6.3.2 Auszuführende Schritte

So führen Sie eine Wiederherstellung zu einer manuell erstellten virtuellen Maschine durch

1. [Bei Wiederherstellung von Windows] Bereiten Sie die Windows-Treiber vor (S. 129), die zu der als Ziel dienenden Virtualisierungsplattform passen.

   Bei unter Linux laufenden Maschinen sind die benötigten Treiber normalerweise bereits im Betriebssystem vorhanden.
2. Erstellen Sie ein bootfähiges Medium (S. 190) mit der Universal Restore-Funktionalität, indem Sie den Acronis Bootable Media Builders verwenden.
3. Erstellen Sie eine virtuelle Maschine, indem Sie die systemeigenen Tools Ihres Virtualisierungsproduktes verwenden.
4. Booten Sie die virtuelle Maschine mit dem bootfähigen Medium.
5. [Bei Wiederherstellung von Windows] Sollten Sie dynamische Volumes benötigen, dann erstellen Sie mithilfe der Funktionen zur Laufwerksverwaltung (S. 215) eine Volume-Gruppe.
6. Wählen Sie die Befehle **Aktionen** –> **Recovery**. Bei Konfiguration einer Wiederherstellung:
   - Aktivieren Sie Universal Restore für Linux oder Universal Restore für Windows. Stellen Sie im letzteren Fall die Treiber bereit, die Sie vorbereitet haben.
   - [Bei Wiederherstellung von Windows] Falls Sie logische Volumes benötigen, dann klicken Sie bei Konfiguration der Wiederherstellung auf **RAID/LVM anwenden**. Die LVM-Struktur wird während der Wiederherstellung automatisch neu erstellt.
7. Konfigurieren Sie andere Recovery-Einstellungen und führen Sie eine Wiederherstellung genauso wie auf eine physikalische Maschine aus.

7 Speicherung der gesicherten Daten

7.1 Depots

Ein Depot ist ein Ort zum Speichern von Backup-Archiven. Zur leichteren Nutzung und Administration ist ein Depot mit den Metadaten der Archive assoziiert. Auf diese Metadaten Bezug zu nehmen, macht Aktionen mit im Depot gespeicherten Archiven und Backups schneller und bequemer.

Ein Depot kann auf einem lokalen Laufwerk, auf einem Netzlaufwerk oder auf einem entfernbaren Medium organisiert werden.

Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung begrenzen, aber die Gesamtgröße aller Archive in einem Depot wird nur durch die Größe des Speichers selbst begrenzt.

Warum sollten Sie ein Depot erstellen?

Es wird empfohlen, dass Sie ein Depot an jedem Zielort erstellen, wo Sie Backup-Archive speichern werden. Das erleichtert Ihre Arbeit auf folgende Weise.

Schneller Zugriff auf ein Depot

Sie müssen sich niemals Pfade zu Ordnern merken, in denen die Archive gespeichert werden. Beim Erstellen eines Backup-Plans oder eines Tasks, der die Wahl eines Archivs bzw. eines Archiv-Zielortes benötigt, ist die Depot-Liste zum schnellen Zugriff verfügbar, damit Sie den Verzeichnisbaum nicht durchsuchen müssen.

Leichte Verwaltung der Archive

Sie können auf ein Depot aus dem Fensterbereich **Navigation** zugreifen. Wenn Sie ein Depot ausgewählt haben, können Sie die dort gespeicherten Archive durchsuchen und mit ihnen folgende Verwaltungsaktionen durchführen:

- Eine Liste der in jedem Archiv enthaltenen Backups abfragen
- Daten aus einem Backup wiederherstellen
- Den Inhalt eines Backups untersuchen
- Alle oder bestimmte Archive bzw. Backups in dem Depot validieren
- Ein Volume-Backup mounten, um Dateien aus dem Backup auf ein physikalisches Laufwerk zu kopieren
- Archive bzw. Backups aus Archiven sicher löschen.

Die Erstellung von Depots ist zwar sehr empfehlenswert, aber nicht obligatorisch. Sie können auf die Verwendung von Verknüpfungen verzichten und stattdessen immer den Pfad zum Speicherort angeben.

Die Erstellung eines Depots führt schließlich dazu, dass sein Name zum Abschnitt **Depots** im Fensterbereich **Navigation** hinzugefügt wird.

Ansicht 'Depots'

Depots (im Fensterbereich 'Navigation') – oberstes Element des Verzeichnisbaums 'Depots'. Klicken Sie auf dieses Element, um persönliche Depots anzuzeigen. Verwenden Sie die im oberen

Bereich der Ansicht **Depots** liegende Symbolleiste, um Aktionen auf ein Depot anzuwenden. Siehe den Abschnitt 'Aktionen für persönliche Depots (S. 164)'.

Persönliche Depots. Diese Depots sind verfügbar, wenn die Konsole mit einer verwalteten Maschine verbunden ist. Klicken Sie auf ein Depot im Depot-Verzeichnisbaum, um eine Detailansicht dieses Depots (S. 163) zu öffnen und führen Sie dann Aktionen mit den dort gespeicherten Archiven (S. 185) und Backups (S. 185) aus.

7.1.1 Mit Depots arbeiten

Dieser Abschnitt beschreibt kurz die Hauptelemente der Benutzeroberfläche für ein ausgewähltes Depot und macht Vorschläge, wie Sie damit arbeiten können.

Informationen über ein Depot ermitteln

Die Informationen über ein bestimmtes Depot befinden sich im oberen Fensterbereich eines angewählten Depots. Durch Verwendung der gestapelten Symbolleiste können Sie die Auslastung des Depots abschätzen. Die Auslastung des Depots entspricht dem Verhältnis von freiem und belegtem Speicherplatz im Depot (nicht verfügbar, falls sich das Depot auf einer Bandbibliothek befindet). Der freie Speicherplatz entspricht dem Speicherplatz des Speichergeräts, auf dem sich das Depot befindet. Wenn das Depot beispielsweise auf einem Festplattenlaufwerk liegt, dann entspricht der freie Speicherplatz des Depots dem freien Platz dieses entsprechenden Volumes. Der belegter Speicherplatz entspricht der Gesamtgröße aller Backup-Archive und ihrer Metadaten, sofern in dem Depot vorliegend.

Sie können außerdem die Gesamtzahl aller in diesem Depot gespeicherter Archive und Backups erhalten – sowie den vollständigen Pfad zum Depot.

Durchsuchen des Depot-Inhalts und Datenauswahl

Sie können zum Durchsuchen des Depot-Inhalts sowie zur Auswahl von Daten für eine Wiederherstellung die Registerlaschen **Datenanzeige** oder **Archiv-Anzeige** verwenden.

Datenanzeige
In der Registerkarte **Datenanzeige** werden alle gesicherten Daten anhand nach Versionen durchsucht und ausgewählt (Backup-Datum und - Zeit). Die Registerlasche **Datenanzeige** teilt sich die Funktionalität zur Suche und Katalogisierung mit dem Datenkatalog (S. 116).

Archiv-Anzeige
In der Registerlasche **Archiv-Anzeige** werden die gesicherten Daten nach Archiven angezeigt. Verwenden Sie die **Archiv-Anzeige**, um Aktionen mit im Depot gespeicherten Archiven und Backups durchzuführen. Zu weiteren Informationen über diese Aktionen siehe folgende Abschnitte:

- 'Aktionen mit im Depot gespeicherten Archiven (S. 185)'.
- 'Aktionen mit Backups (S. 185)'.
- 'Tabellenelemente sortieren, filtern und konfigurieren (S. 18)'.

Welche Bedeutung hat das Symbol ?

Beim Durchsuchen von Archiven in der Registerkarte **Archiv-Anzeige** fällt Ihnen möglicherweise ein Backup mit dem Symbol auf. Dieses Symbol bedeutet, dass das Backup zum Löschen gekennzeichnet ist, aber nicht sofort gelöscht wurde, weil noch andere Backups von diesem abhängen und eine Konsolidierung nicht möglich ist oder durch die Aufbewahrungsregeln deaktiviert ist.

Sie können keine Aktionen mit solchen Backups durchführen, die zum Löschen gekennzeichnet sind. Sie verschwinden aus der **Archiv-Anzeige**, nachdem Sie physikalisch gelöscht wurden. Dazu kommt es, wenn auch alle abhängigen Backups gelöscht wurden oder nach der nächsten Bereinigung, nachdem Sie in den Aufbewahrungsregeln die Konsolidierung aktiviert haben.

7.1.2 Persönliche Depots

Ein Depot wird als persönlich bezeichnet, wenn es durch direkte Verbindung der Konsole zu einer verwalteten Maschine erstellt wurde. Persönliche Depots sind spezifisch für jede verwaltete Maschine. Persönliche Depots sind für jeden Benutzer sichtbar, der sich am System anmelden kann. Die Berechtigungen eines Benutzers, Backups zu einem persönlichen Depot durchzuführen, werden über die Zugriffsrechte definiert, die dieser Benutzer für den Ordner bzw. das Gerät hat, wo das Depot gespeichert ist.

Ein persönliches Depot kann auf Netzwerkfreigaben, FTP-Servern, auf trenn- bzw. wechselbaren Medien, im Acronis Cloud Storage, auf Bandgeräten oder auf einem für die Maschine lokalen Laufwerk organisiert werden. Die Acronis Secure Zone wird als persönliches Depot betrachtet, das für alle Benutzer verfügbar ist, die sich am System anmelden können. Persönliche Depots werden automatisch erstellt, wenn Sie Backups zu einem der oberen Speicherorte durchführen.

Persönliche Depots können von lokalen Backup-Plänen bzw. Tasks verwendet werden.

Persönliche Depots erstellen

Mehrere Maschinen können sich auf denselben physikalischen Speicherort beziehen, beispielsweise auf denselben freigegebenen Ordern. Jede dieser Maschinen hat im Verzeichnisbaum **Depots** jedoch ihre eigene Verknüpfung. Benutzer, die ein Backup zu einem gemeinsam genutzten Ordner durchführen, können die Archive anderer Benutzer sehen und verwalten, abhängig von ihren Zugriffsberechtigungen für diesen Ordner. Um die Identifikation von Archiven zu erleichtern, hat die Ansicht **Persönliches Depot** die Spalte **Besitzer**, die den Besitzer eines jeden Archivs zeigt. Um mehr über das Konzept der Besitzer zu erfahren, siehe Besitzer und Anmeldedaten (S. 23).

Metadaten

In jedem persönlichen Depot wird bei Backup-Durchführung ein Ordner namens **.meta** erstellt. Dieser Ordner enthält zusätzliche Informationen über die im Depot gespeicherten Archive und Backups, wie z.B. die Besitzer der Archive oder den Maschinen-Namen. Sollten Sie den .meta-Ordner einmal versehentlich löschen, dann wird er automatisch neu erstellt, sobald Sie das nächste Mal auf das Depot zugreifen. Einige Informationen, wie Besitzer- oder Maschinen-Namen, können jedoch verloren gehen.

7.1.2.1 Auf persönliche Depots anwendbare Aktionen

Klicken Sie, um auf Aktionen für persönliche Depots zugreifen zu können, im Fensterbereich **Navigation** auf **Depots** –> **Persönlich**.

Alle hier beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Depot-Symbolleiste ausgeführt. Sie können auf diese Aktionen auch über das Hauptmenüelement **[Depot-Name] Aktionen** zugreifen.

Anleitung zur Durchführung von Aktionen mit persönlichen Depots.

Aufgabe	Lösung
Persönliche Depots erstellen	Klicken Sie auf **Erstellen**. Die Prozedur zum Erstellen persönlicher Depots wird ausführlich im Abschnitt Ein persönliches Depot erstellen (S. 165) beschrieben.
Ein Depot bearbeiten	1. Wählen Sie das Depot. 2. Klicken Sie auf **Bearbeiten**. Auf der Seite **Persönliches Depot bearbeiten** können Sie den Depotnamen sowie die Informationen im Feld **Kommentare** bearbeiten.
Benutzerkonto für den Zugriff auf ein Depot ändern	Klicken Sie auf **Benutzer ändern**. Geben Sie im erscheinenden Dialogfenster die für den Zugriff auf das Depot benötigten Anmeldedaten ein.
Acronis Secure Zone erstellen	Klicken Sie auf **Acronis Secure Zone erstellen**. Die Prozedur zur Erstellung der Acronis Secure Zone ist ausführlich im Abschnitt Acronis Secure Zone erstellen (S. 167) erläutert.
Den Inhalt eines Depots durchsuchen	Klicken Sie auf **Durchsuchen**. Untersuchen Sie den gewählten Depot-Inhalt im erscheinenden Explorer-Fenster.
Ein Depot validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite Validierung (S. 172) mit dem bereits als Quelle vorausgewählten Depot. Die Validierung des Depots überprüft alle in diesem Ordner gespeicherten Archive.
Ein Depot löschen	Klicken Sie auf **Löschen**. Tatsächlich entfernt die Löschaktion aus der Ansicht **Depots** nur die Verknüpfung zum entsprechenden Ordner. Der Ordner selbst bleibt unberührt. Sie haben die Möglichkeit, die im Ordner enthaltenen Archive zu behalten oder zu löschen.
Die Informationen der Depot-Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Während Sie den Inhalt eines Depots einsehen, können Archive dem Depot hinzugefügt, aus diesem gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, damit die neuesten Veränderungen für die Depot-Informationen berücksichtigt werden.

Ein persönliches Depot erstellen

So erstellen Sie ein persönliches Depot

1. Geben Sie im Feld **Name** die Bezeichnung für das zu erstellende Depot ein.
2. [Optional] Geben Sie im Feld **Kommentare** eine Beschreibung für das Depot ein.
3. Klicken Sie auf **Pfad** und spezifizieren Sie einen Pfad zu dem Ordner, der als Depot verwendet werden soll. Ein persönliches Depot kann auf Netzwerkfreigaben, FTP-Servern, entfernbaren Medien, im Acronis Cloud Storage, auf Bandgeräten oder auf einem für die Maschine lokalen Laufwerk organisiert werden.
4. [Optional] Falls das Depot auf einem Bandgerät erstellt wird:
    a. Klicken Sie auf **Laufwerke**, um das/die Bandlaufwerk(e) zu spezifizieren, welche(s) bei Backups zum Depot verwendet werden sollen. Standardmäßig werden alle verfügbaren

Laufwerke verwendet. Klicken Sie auf **Nur die folgenden Laufwerke verwenden** und (de)aktivieren Sie die gewünschten Kontrollkästchen;

   b. Klicken Sie auf **Band-Pool** und spezifizieren Sie den Pool, dessen Bänder von dem Depot verwendet werden sollen. Standardmäßig ist der Pool **Acronis** vorausgewählt.

5. Klicken Sie auf **OK**. Als Ergebnis erscheint das erstellte Depot in der Gruppe **Persönlich** des Depot-Verzeichnisbaums.

Persönliche Depots zusammenführen und verschieben

Was ist, wenn ich ein existierendes Depot von einem Ort zu einem anderen verschieben muss?

Verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das betreffende Depot beim Verschieben der Dateien verwendet – oder deaktivieren Sie die entsprechenden Pläne. Siehe den Abschnitt 'Aktionen für Backup-Pläne und Tasks (S. 249)'.
2. Verschieben Sie den Depot-Ordner mit seinem kompletten Inhalt manuell, unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Ein neues Depot erstellen.
4. Bearbeiten Sie die Backup-Pläne und Tasks: Stellen Sie ihre Zielortangaben auf das neue Depot um.
5. Löschen Sie das alte Depot.

Wie kann ich zwei Depots zusammenführen?

Angenommen, Sie benutzen zwei Depots *A* und *B*. Beide Depots werden von Backup-Plänen verwendet. Sie entscheiden, nur Depot *B* zu behalten, indem Sie alle Archive aus Depot *A* dorthin verschieben.

Zur Umsetzung verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das Depot *A* während der Zusammenführung verwendet – oder deaktivieren Sie die betreffenden Pläne temporär. Siehe den Abschnitt 'Aktionen für Backup-Pläne und Tasks (S. 249)'.
2. Verschieben Sie den Inhalt des Depots *A* manuell zum Depot *B* unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Bearbeiten Sie die Backup-Pläne, die das Depot *A* benutzen: Stellen Sie die Zielortangaben auf Depot *B* um.
4. Wählen Sie im Depot-Verzeichnisbaum das Depot *B* aus, um zu überprüfen, dass die Archive angezeigt werden. Wenn nicht, klicken Sie auf **Aktualisieren**.
5. Löschen Sie das Depot *A*.

7.2 Acronis Secure Zone

Die Acronis Secure Zone ist ein sicheres Volume auf dem Laufwerksspeicherplatz einer verwalteten Maschine, in der Backup-Archive hinterlegt werden können, so dass die Wiederherstellung eines Laufwerks auf demselben Laufwerk erfolgen kann, auf dem sich auch die Backups selbst befinden.

Sollte das Laufwerk jedoch einen physikalischen Fehler haben, so gehen die Zone und alle dort aufbewahrten Archive verloren. Das ist der Grund, warum die Acronis Secure Zone nicht der einzige Ort sein sollte, wo Backups gespeichert werden. In Unternehmensumgebungen kann die Acronis Secure Zone als Zwischenspeicher für Backups betrachtet werden, wenn der üblicherweise

verwendete Speicherort temporär nicht verfügbar ist oder über einen langsamen bzw. ausgelasteten Kanal angebunden ist.

Vorteile

Acronis Secure Zone:

- Ermöglicht die Wiederherstellung eines Laufwerks (wie einer Festplatte) zu demselben Laufwerk, auf dem die Laufwerk-Backups selbst hinterlegt sind.
- Bietet eine kosteneffektive und handliche Methode zum Schutz Ihrer Daten vor Softwarefehlern, Virusangriffen, Bedienungsfehlern u.a.
- Da es ein interner Archiv-Speicher ist, beseitigt er die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders nützlich für mobile Benutzer.
- Kann als primäres Backup-Ziel dienen, wenn die Funktion Replikation von Backups (S. 81) verwendet wird.

Einschränkungen

- Die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk organisiert werden.

7.2.1 Acronis Secure Zone erstellen

Sie können die Acronis Secure Zone erstellen, während das Betriebssystem läuft oder Sie ein bootfähiges Medium benutzen.

Zur Erstellung der Acronis Secure Zone führen Sie die folgenden Schritte aus.

Speicherort und Größe

Laufwerk (S. 167)

Wählen Sie (sofern mehrere vorhanden sind) eine fest eingebaute Festplatte (oder ähnliches Laufwerk), auf dem die Zone erstellt werden soll. Die Acronis Secure Zone wird unter Verwendung von nicht zugeordnetem Speicherplatz oder auf Kosten freien Speicherplatzes der Partition erstellt.

Größe (S. 168)

Spezifizieren Sie die exakte Größe der Zone. Verschieben oder Größenveränderung einer gesperrten Partition, wie der aktuellen Betriebssystempartition, benötigen einen Neustart.

Sicherheit

Kennwort (S. 168)

[Optional] Schützen Sie die Acronis Secure Zone vor unerlaubtem Zugriff mit einem Kennwort. Das Kennwort wird bei jeder die Zone betreffende Aktion erfragt.

Klicken Sie auf OK, nachdem Sie die benötigten Einstellungen konfiguriert haben. Überprüfen Sie im Fenster Ergebnisbestätigung (S. 168) das erwartete Layout und klicken Sie auf OK, um die Erstellung der Zone zu starten.

7.2.1.1 Acronis Secure Zone Laufwerk

Die Acronis Secure Zone kann auf jeder fest installierten Festplatte (oder ähnlichem Laufwerk) liegen. Die Acronis Secure Zone wird immer am Ende des Laufwerks eingerichtet. Eine Maschine kann jedoch nur eine Acronis Secure Zone haben. Die Acronis Secure Zone wird unter Verwendung von 'nicht zugeordnetem' Speicherplatz oder auf Kosten freien Speicherplatzes der Volumes erstellt.

Die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk organisiert werden.

So weisen Sie der Acronis Secure Zone Speicherplatz zu

1. Wählen Sie (sofern mehrere vorhanden sind) eine fest eingebaute Festplatte (oder ähnliches Laufwerk), auf dem die Zone erstellt werden soll. Standardmäßig wird der 'nicht zugeordnete' sowie freie Speicherplatz aller Volumes des ersten aufgelisteten Laufwerks gewählt. Das Programm zeigt den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an.
2. Wenn Sie der Zone mehr Speicherplatz zuweisen müssen, können Sie Volumes wählen, von denen freier Platz übernommen werden soll. Das Programm zeigt erneut den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an, basierend auf Ihrer Auswahl. Sie können die exakte Größe der Zone im Fenster **Acronis Secure Zone Größe** (S. 168) einstellen.
3. Klicken Sie auf **OK**.

7.2.1.2 Acronis Secure Zone Größe

Geben Sie die Größe der Acronis Secure Zone ein oder ziehen Sie am Schieber, um eine Größe zwischen der minimalen und maximalen zu wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte. Die maximale Größe entspricht dem nicht zugeordneten Festplattenplatz plus dem gesamten freien Platz aller im vorherigen Schritt gewählten Partitionen.

Beachten Sie Folgendes, wenn Sie Speicherplatz von der Boot- bzw. System-Partition verwenden müssen:

- Ein Verschieben oder eine Größenänderung der Partition, von der das System gegenwärtig bootet, verlangen einen Neustart.
- Die Verwendung des gesamten freien Speichers einer Systempartition kann dazu führen, dass das Betriebssystem instabil wird oder sogar nicht mehr startet. Stellen Sie also nicht die maximale Größe für die Zone ein, falls Sie die Boot- bzw. System-Partition gewählt haben.

7.2.1.3 Kennwort für die Acronis Secure Zone

Die Vergabe eines Kennwortes schützt die Acronis Secure Zone vor unerlaubtem Zugriff. Das Programm wird bei allen Aktionen, die die Zone und dort gespeicherte Archive betreffen, nach dem Kennwort fragen – wie etwa Backup und Wiederherstellung, Archiv-Validierung, Größenveränderung und Löschen der Zone.

So vergeben Sie ein Kennwort

1. Wählen Sie **Kennwort verwenden**.
2. Tippen Sie das neue Kennwort in das Feld **Kennwort eingeben** ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Klicken Sie auf **OK**.

So deaktivieren Sie ein Kennwort

1. Wählen Sie **Nicht verwenden**.
2. Klicken Sie auf **OK**.

7.2.1.4 Ergebnisbestätigung

Das Fenster **Ergebnisbestätigung** zeigt das erwartete Partitionslayout entsprechend der von Ihnen gewählten Einstellungen. Klicken Sie auf **OK**, falls Sie mit dem Layout einverstanden sind, worauf die Erstellung der Acronis Secure Zone startet.

So werden die Einstellungen umgesetzt

Die nachfolgende Erläuterung hilft Ihnen zu verstehen, welche Auswirkung die Erstellung der Acronis Secure Zone auf eine Festplatte hat, die mehrere Partitionen enthält.

- Die Acronis Secure Zone wird immer am Ende der Festplatte eingerichtet. Bei Kalkulation des endgültigen Partitionslayouts wird das Programm zuerst nicht zugeordneten, am Ende liegenden Festplattenplatz verwenden.
- Sollte der nicht zugeordnete Speicherplatz am Ende der Festplatte nicht ausreichen, jedoch zwischen den Partitionen noch nicht zugeordneter Speicherplatz vorhanden sein, so werden die Partitionen verschoben, um dem Endbereich mehr nicht zugeordneten Speicherplatz hinzuzufügen.
- Wenn dann der zusammengetragene nicht zugeordnete Speicherplatz immer noch nicht ausreicht, wird das Programm freien Speicherplatz von Partitionen beziehen, die Sie auswählen und deren Größe proportional verkleinern. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.
- Auf einem Laufwerk sollte jedoch genügend freier Platz vorhanden sein, so dass Betriebssystem und Anwendungen arbeitsfähig sind, z.B. zum Erstellen temporärer Dateien. Das Programm wird keine Partition verkleinern, deren freier Speicherplatz dadurch kleiner als 25% der Gesamtgröße wird. Nur wenn alle Partitionen der Festplatte mindestens 25% freien Speicherplatz haben, wird das Programm mit der proportionalen Verkleinerung der Partitionen fortfahren.

Daraus wird ersichtlich, dass es nicht ratsam ist, für die Zone die maximal mögliche Größe einzustellen. Sie haben am Ende dann auf keinem Laufwerk mehr freien Speicherplatz, was dazu führen kann, dass Betriebssystem und Anwendungen instabil arbeiten oder nicht mehr starten.

7.2.2 Die Acronis Secure Zone verwalten

Die Acronis Secure Zone wird als persönliches Depot (S. 298) betrachtet. Einmal auf einer verwalteten Maschine erstellt, ist die Zone stets in der Liste **Persönliche Depots** präsent.

Alle für Depots verfügbaren Aktionen zur Archiv-Verwaltung sind auch auf die Acronis Secure Zone anwendbar. Zu weiteren Informationen über Archiv-Verwaltungsaktionen siehe den Abschnitt 'Aktionen mit Archiven und Backups (S. 184)'.

7.2.2.1 Acronis Secure Zone vergrößern

So vergrößern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Vergrößern**.
2. Bestimmen Sie die Volumes, deren freier Speicher zur Vergrößerung der Acronis Secure Zone verwendet werden soll.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:
   - am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und dem maximalen Wert wählen. Die maximale Größe entspricht dem nicht zugeordneten Festplattenspeicherplatz plus dem gesamten freien Speicher aller gewählten Partitionen;
   - einen exakten Wert für die Größe der Acronis Secure Zone eingeben.

   Bei Vergrößerung der Zone verfährt das Programm wie folgt:

   - Zuerst wird es den nicht zugeordneten Festplattenspeicherplatz benutzen. Falls notwendig, werden Partitionen verschoben, jedoch nicht in ihrer Größe verändert. Das Verschieben einer gesperrten Partition benötigt einen Neustart.

- Sollte nicht genügend nicht zugeordneter Speicher vorhanden sein, so wird das Programm freien Speicherplatz von den ausgewählten Partitionen beziehen, deren Größe dabei proportional verkleinert wird. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.

Die Verkleinerung einer Systempartition auf ihre minimale Größe kann das Betriebssystem der Maschine am Booten hindern.

4. Klicken Sie auf **OK**.

7.2.2.2 Die Acronis Secure Zone verkleinern

So verkleinern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Verkleinern**.
2. Bestimmen Sie Volumes, die den frei werdenden Speicherplatz nach Verkleinerung der Zone zugesprochen bekommen.

   Der Speicherplatz wird gleichmäßig auf die entsprechenden Volumes verteilt, sofern Sie mehrere ausgewählt haben. Der freigegebene Bereich wird zu 'nicht zugeordneten' Speicherplatz, wenn Sie keine Volumes auswählen.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:
   - am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und minimalen Wert wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte.
   - einen exakten Wert im Feld **Acronis Secure Zone Größe** eingeben.
4. Klicken Sie auf **OK**.

7.2.2.3 Eine Acronis Secure Zone löschen

So löschen Sie eine Acronis Secure Zone:

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf den Befehl **Löschen**.
2. Wählen Sie im Fenster **Acronis Secure Zone löschen** diejenigen Volumes, denen Sie den durch die Zone freigegebenen Platz zuweisen wollen – klicken Sie anschließend auf **OK**.

   Der Speicherplatz wird gleichmäßig auf die entsprechenden Volumes verteilt, sofern Sie mehrere ausgewählt haben. Der freigegebene Bereich wird zu 'nicht zugeordneten' Speicherplatz, wenn Sie keine Volumes auswählen.

Nachdem Sie auf **OK** geklickt haben, beginnt Acronis Backup mit der Löschung der Zone.

7.3 Wechsellaufwerke

In diesem Abschnitt werden Besonderheiten beim Backup auf Wechsellaufwerke beschrieben.

Mit Wechsellaufwerk werden hier RDX- oder USB-Flash-Laufwerke (z.B. USB-Sticks) gemeint. Eine USB-Festplatte wird nicht als Wechsellaufwerk angesehen, außer es wird als solches vom Betriebssystem erkannt.

Unter Linux wird ein RDX- oder USB-Flash-Laufwerk als Wechsellaufwerk angesehen, wenn es über seinen Namen spezifiziert wird (beispielsweise **sdf:/**). Wird ein Laufwerk über seinen Mount-Punkt (beispielsweise **/mnt/backup**) spezifiziert, dann verhält es sich wie ein fest eingebautes Laufwerk.

Die Methode, nach der mit Wechselaufwerk-Bibliotheken (Multi-Cartridge-Geräte) gearbeitet wird, hängt vom Gerätetyp, dem Hersteller und der Konfiguration ab. Daher sollte jeder Fall individuell betrachtet werden.

Depots auf Wechsellaufwerken

Bevor Sie eine Maschine auf ein Wechsellaufwerk sichern, können Sie ein persönliches Depot erstellen (S. 165). Falls Sie nicht wollen, wird die Software automatisch ein persönliches Depot in dem für das Backup ausgewählten Laufwerksordner erstellen.

Beschränkung

- Auf Wechsellaufwerken erstellte Depots haben keine Registerkarte **Datenanzeige** (S. 116).

Betriebsmodi von Wechsellaufwerken

Sie können bei Erstellung eines Backup-Plans (S. 38) wählen, ob Ihr Wechsellaufwerk als eingebautes Laufwerk oder wie ein Wechselmedium verwendet wird. Der Modus **Eingebautes Laufwerk** nimmt an, dass das Wechsellaufwerk immer an die Maschine angeschlossen sein wird. Der Modus **Wechselmedium** ist als Standard vorausgewählt.

Beim Backup unter Verwendung der Funktion **Backup jetzt** oder unter einem bootfähigen Medium wird das Wechsellaufwerk immer im Modus **Wechselmedium** verwendet.

Der Unterschied zwischen diesen beiden Modi liegt hauptsächlich bei den Funktionen für Aufbewahrung und Replikation von Backups.

Funktionalität	Eingebautes Laufwerk	Wechselmedium
Falls der Speicherplatz zur Fortsetzung des Backups nicht ausreicht, wird die Software Sie auffordern:	...Speicherplatz manuell freizugeben.	...ein neues Medium einzulegen.
Sie können für die auf dem Gerät gespeicherten Backups Aufbewahrungsregeln (S. 82) einrichten.	Ja	Nein
Sie können zur Bereinigung des Archivs die Option '**Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist**' innerhalb des Backup-Schemas **Benutzerdefiniert** (S. 51) einrichten.	Ja	Nein
Vereinfachte Benennung (S. 61) von Backup-Dateien...	...ist nicht verfügbar.	...wird immer verwendet.
Das Replizieren von Backups (S. 81) *zu* einem Wechsellaufwerke ist möglich.	Ja	Nein
Sie können Backups auch *von* einem Wechsellaufwerk aus replizieren.	Nein	Nein
Ein Archiv mit mehreren Voll-Backups kann erstellt werden.	Ja	Nein. Die Software löscht vor Erstellung eines neuen Voll-Backups das komplette Archiv und startet danach ein neues.
Sie können jedes Backup eines Archivs löschen.	Ja	Nein. Sie können nur ein Backup löschen, welches keine abhängigen Backups hat.

Da der Wechsellaufwerksmodus das Benennungsschema für Backup-Dateien bestimmt, erscheint das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht, wenn es sich beim Backup-Ziel um ein Wechsellaufwerk handelt.

8 Aktionen mit Archiven und Backups

8.1 Archive und Backups validieren

Validierung ist eine Aktion, mit der die Möglichkeit der Datenwiederherstellung aus einem Backup geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Festplatten- oder Partitions-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Beide Prozeduren sind ressourcenintensiv.

Die Validierung eines Archivs bestätigt die Gültigkeit aller Backups im Archiv. Die Validierung eines Depots (bzw. Speicherorts) bewirkt eine Überprüfung aller in diesem Depot (Speicherort) hinterlegten Archive.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie ein Betriebssystem gesichert haben und Sie sichergehen wollen, dass spätere Recovery-Aktionen des Backups erfolgreich sind, dann lässt sich das nur garantieren, wenn Sie eine testweise Wiederherstellung unter Verwendung einer bootfähigen Umgebung auf ein freies, ungenutztes Laufwerk durchführen. Sie sollten zumindest sicherstellen, dass das Backup unter Verwendung eines bootfähigen Mediums erfolgreich validiert werden kann.

Beschränkung
Archive und Backups im Acronis Cloud Storage (S. 271) können nicht validiert werden. Ein 'Initial Seeding'-Backup (S. 275) wird jedoch direkt nach seiner Erstellung automatisch validiert.

Verschiedene Varianten, einen Validierungstask zu erstellen

Die Verwendung der Seite **Validation** ist der übliche Weg, um einen Validierungstask zu erstellen. Sie können hier Validierungen sofort ausführen oder eine Validierungsplanung für jedes Backup, Archiv oder Depot erstellen, auf das Sie Zugriff haben.

Die Validierung eines Archivs oder des letzten Backups in dem Archiv kann auch als Teil eines Backup-Plans durchgeführt werden. Weitere Informationen finden Sie im Abschnitt 'Einen Backup-Plan erstellen (S. 38)'.

Wählen Sie zuerst ein Objekt zur Validierung aus, um Zugriff auf die Seite **Validierung** zu erhalten: ein Depot, ein Archiv oder ein Backup.

- Klicken Sie zur Wahl eines Depots im Fensterbereich **Navigation** auf das Symbol **Depots** – und wählen Sie dann das Depot, indem Sie den Depot-Verzeichnisbaum in der Ansicht **Depots** erweitern oder es direkt im Fensterbereich **Navigation** auswählen.
- Wählen Sie zur Auswahl eines Archivs zuerst ein Depot an und dann in der Ansicht **Depot** die Registerlasche **Archiv-Anzeige** – anschließend klicken Sie auf den Namen des entsprechenden Archivs.
- Wählen Sie zur Wahl eines Backups zuerst ein Archiv aus der **Archiv-Anzeige**, erweitern Sie dann das Archiv über die entsprechende Schaltfläche links neben dem Archivnamen und klicken Sie abschließend auf das gewünschte Backup.

Klicken Sie nach Wahl des Validierungsobjektes im Kontextmenü auf den Befehl **Validieren**. Darauf öffnet sich die Seite **Validierung** mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch wählen, wann validiert werden soll, und (optional) einen Namen für den Tasks angeben.

Zur Erstellung eines Validierungstasks führen Sie die folgenden Schritte aus.

Validierungsquelle

Validieren

Wählen Sie ein zu validierendes Objekt:

Archiv (S. 178) – Sie müssen in diesem Fall das Archiv spezifizieren.

Backup (S. 174) - spezifizieren Sie zuerst das Archiv. Wählen Sie dann das gewünschte Backup aus dem Archiv.

Depot (S. 174) – wählen Sie ein Depot (oder einen anderen Speicherort), dessen Archive validiert werden sollen.

Anmeldedaten (S. 174)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat.

Validierungszeitpunkt

Validierung starten (S. 175)

Geben Sie an, wann und wie oft die Validierung durchgeführt werden soll.

Task-Parameter

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Validierungstask ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Anmeldedaten des Plans: (S. 175)

[Optional] Der Validierungstask wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Anmeldedaten für den Task ändern.

Kommentare

[Optional] Geben Sie Kommentare für den Task ein.

Nachdem Sie alle notwendigen Einstellungen konfiguriert haben, klicken Sie auf **OK**, um den Validierungstask zu erstellen.

8.1.1 Auswahl des Archivs

So spezifizieren Sie ein zu validierendes Archiv

1. Tragen Sie den vollständigen Pfad zum Archiv-Speicherort in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum (S. 115).
2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die sich in jedem von Ihnen gewählten Speicherort befinden.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.
3. Klicken Sie auf **OK**.

8.1.2 Auswahl der Backups

So spezifizieren Sie ein zu validierendes Backup.

1. Wählen Sie im oberen Fensterbereich ein Backup anhand des Zeitstempels.

   Der untere Teil des Fensters zeigt den Inhalt des gewählten Backups, um Sie darin zu unterstützen, das richtige Backup herauszufinden.

2. Klicken Sie auf **OK**.

8.1.3 Depot wählen

So wählen Sie ein Depot oder einen Speicherort

1. Tragen Sie den vollständigen Pfad zum Depot (Speicherort) in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum.

- Um ein zentrales Depot auszuwählen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
- Um ein persönliches Depot auszuwählen, erweitern Sie die Gruppe **Persönlich** und klicken dann auf das entsprechende Depot.
- Um einen lokalen Ordner auszuwählen (CD-/DVD-Laufwerk oder ein lokal angeschlossenes Bandgerät), erweitern Sie die Gruppe **Lokale Ordner** und klicken auf den gewünschten Ordner.
- Um eine Netzwerkfreigabe zu wählen, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
- Um einen Ordner auszuwählen, der auf einer NFS-Freigabe gespeichert ist, erweitern Sie die Gruppe **NFS-Laufwerke** und klicken Sie auf den entsprechenden Ordner.
- Um einen **FTP-** oder **SFTP-**Server zu wählen, erweitern Sie die korrespondierende Gruppe und wählen die entsprechenden Ordner auf dem Server.

  Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

  Die Tabelle zeigt für jedes von Ihnen gewählte Depot die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Depots zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

1. Klicken Sie auf **OK**.

8.1.4 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert ist.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Die Software greift auf den Speicherort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

Die Software greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

Spezifizieren Sie:

- **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
- **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.1.5 Validierungszeitpunkt

Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu planen, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Bevorzugen Sie es dagegen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, so sollten Sie erwägen, die Validierung direkt nach der Task-Erstellung zu starten.

Wählen Sie eine der folgenden Optionen:

- **Jetzt** – um den Validierungs-Tasks direkt nach seiner Erstellung zu starten, sobald Sie also auf der Validierungs-Seite auf OK geklickt haben.
- **Später** – um einen einmaligen Validierungs-Task zu starten, zu dem von Ihnen angegeben Datum/Zeitpunkt.

  Spezifizieren Sie die passenden Parameter wie folgt:

  - **Datum und Zeit** – das Datum und die Uhrzeit, wann der Task gestartet werden soll.
  - **Task wird manuell gestartet (keine Planung)** – aktivieren Sie dieses Kontrollkästchen, falls Sie den Task später manuell starten wollen.
- **Nach Planung** – um den Task zu planen. Um mehr über die Konfiguration der Planungs-Parameter zu lernen, schauen Sie in den Abschnitt Planung (S. 66).

8.1.6 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten verwenden**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:

    - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
    - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Zu weiteren Informationen über die Verwendung von Anmeldedaten in Acronis Backup siehe den Abschnitt Besitzer und Anmeldedaten (S. 23).

Siehe den Abschnitt 'Benutzerberechtigungen auf einer verwalteten Maschine (S. 25)', um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

8.2 Archive und Backups exportieren

Beim Export wird eine Kopie des Archivs bzw. eine unabhängige Teilkopie des Archivs am von Ihnen angegebenen Speicherort erstellt. Das ursprüngliche Archiv bleibt unverändert.

Ein Export ist möglich für:

- **Ein einzelnes Archiv** – es wird eine exakte Kopie des Archivs erstellt
- **Ein einzelnes Backup** – es wird ein Archiv erstellt, das aus einem einzelnen vollständigen Backup besteht. Beim Export eines inkrementellen oder differentiellen Backups werden die vorhergehenden Backups bis hin zum letzten vollständigen Backup konsolidiert.
- **Ihre Auswahl von Backups**, die zu demselben Archiv gehören – das resultierende Archiv enthält nur die spezifizierten Backups. Eine Konsolidierung erfolgt nach Bedarf; das resultierende Archiv kann daher Voll-Backups enthalten, aber auch inkrementelle und differentielle Backups.

Einsatzszenarien

Mit einem Export können Sie ausgewählte Backups von einer Reihe inkrementeller Backups trennen, um so die Wiederherstellung zu beschleunigen, auf Wechselmedien und externe Medien zu schreiben, oder für andere Zwecke.

Beispiel. Wenn Sie Daten zu einem Remote-Speicherort über eine instabile Netzwerkverbindung oder bei niedriger Netzwerkbandbreite übertragen (etwa ein Backup durch ein WAN unter Verwendung eines VPN-Zugriffs), dann können Sie das anfängliche Voll-Backup auch auf ein Wechselmedium speichern. Schicken Sie das Medium danach zu dem Remote-Speicherort. Dort wird das Backup dann von diesem Medium zu dem als eigentliches Ziel fungierenden Storage exportiert. Nachfolgende inkrementelle Backups, die üblicherweise deutlich kleiner sind, werden dann per Netzwerk/Internet übertragen.

Beim Export eines verwalteten Depots auf ein Wechselmedium erhalten Sie ein transportierbares, nicht verwaltetes Depot für den Einsatz in folgenden Szenarien:

- Aufbewahrung einer externen Kopie (offsite) Ihres Depots oder der wichtigsten Archive.
- 'Physischer' Transport eines Depots zu einer entfernten Niederlassung.
- Wiederherstellung ohne Zugriff auf den Storage Node bei Netzwerkproblemen oder Ausfall des Storage Nodes.
- Wiederherstellung des Storage Node selbst.

Der Export von einem Festplatten-basierten Depot auf ein Bandgerät kann als einfache Form des 'Archiv-Staging' angesehen werden.

Der Name des resultierenden Archivs

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort.
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt.
- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort.

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

Die Optionen des resultierenden Archivs

Das exportierte Archiv erbt die Optionen des ursprünglichen Archivs einschließlich Verschlüsselung und Kennwort. Beim Export eines kennwortgeschützten Archivs werden Sie zur Eingabe des Kennworts aufgefordert. Wenn das ursprüngliche Archiv verschlüsselt ist, wird mit dem Kennwort auch das resultierende Archiv verschlüsselt.

Aktionen mit einem Export-Task

Ein Export-Task startet sofort, nachdem die Konfiguration abgeschlossen ist. Sie können einen Export-Task wie jeden anderen Task stoppen oder löschen.

Sobald ein Export-Task abgeschlossen wurde, können Sie ihn jederzeit erneut ausführen. Löschen Sie zunächst das aus der letzten Ausführung des Task resultierende Archiv, falls es sich noch im Zieldepot befindet. Anderenfalls wird der Task fehlschlagen. Sie können bei einem Export-Task das Zielarchiv nicht umbenennen (das ist eine Einschränkung).

Tipp: *Dieses Staging-Szenario kann manuell umgesetzt werden, indem Sie immer erst den Task zum Löschen des Archivs und dann den Export-Task ausführen.*

Verschiedene Varianten, einen Export-Task zu erstellen

Gewöhnlich werden Export-Tasks über die Seite **Exportieren** erstellt. Dort können Sie jedes Backup oder Archiv exportieren, auf das Sie Zugriffsrechte besitzen.

Auf die Seite **Exportieren** können Sie aus der Ansicht **Depots** zugreifen. Klicken Sie mit der rechten Maustaste auf das zu exportierende Objekt (Archiv oder Backup) und wählen Sie im Kontextmenü **Exportieren**.

Wählen Sie zuerst ein Validierungsobjekt aus, um Zugriff auf die Seite **Exportieren** zu erhalten: ein Archiv oder ein Backup.

1. Wählen Sie ein Depot. Klicken Sie dazu im Fensterbereich **Navigation** auf das Symbol **Depots** und wählen Sie dann das Depot, indem Sie den Depot-Verzeichnisbaum in der Ansicht **Depots** erweitern oder es direkt im Fensterbereich **Navigation** auswählen.
2. Wählen Sie zur Auswahl eines Archivs zuerst ein Depot an und dann in der Ansicht **Depot** die Registerlasche **Archiv-Anzeige** – anschließend klicken Sie auf den Namen des entsprechenden Archivs.
3. Wählen Sie zur Wahl eines Backups zuerst ein Archiv aus der **Archiv-Anzeige**, erweitern Sie dann das Archiv über die entsprechende Schaltfläche links neben dem Archivnamen und klicken Sie abschließend auf das gewünschte Backup.

Klicken Sie nach Wahl des Validierungsobjektes im Kontextmenü auf den Befehl **Exportieren**. Darauf öffnet sich die Seite **Exportieren** mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch einen Ziel-Speicherort wählen und (optional) einen Namen für den Task angeben.

Führen Sie folgende Schritte aus, um ein Archiv oder ein Backup zu exportieren.

Export-Quelle

Exportieren

Wählen Sie den Typ der zu exportierenden Objekte:

Archiv – in diesem Fall müssen Sie nur das benötigte Archiv spezifizieren.

Backups – Sie müssen zuerst das Archiv spezifizieren und erst danach wählen Sie das/die gewünschten Backup(s) in diesem Archiv.

Durchsuchen

Wählen Sie das **Archiv** (S. 178) oder die **Backups** (S. 179).

Anmeldedaten anzeigen (S. 179)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat.

Export-Ziel

Durchsuchen (S. 179)

Spezifizieren Sie den Pfad zu dem Speicherort, wo das neue Archiv erstellt wird.

Vergeben Sie einen eindeutigen Namen und Kommentar für das neue Archiv.

Vollständige Katalogisierung/Schnelle Katalogisierung

Nicht verfügbar bei bootfähigen Medien oder bei Speicherorten, die keine Katalogisierung unterstützen.

Bestimmen Sie, ob auf die exportierten Backups eine vollständige oder schnelle Katalogisierung durchgeführt werden soll. Weitere Informationen zur Katalogisierung finden Sie im Abschnitt 'Backup-Katalogisierung (S. 91)'.

Anmeldedaten anzeigen (S. 181)

[Optional] Stellen Sie Anmeldedaten für den Ziel-Speicherort zur Verfügung, falls das Benutzerkonto des Tasks nicht ausreichende Zugriffsrechte darauf hat.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Export zu starten.

Als Ergebnis zeigt das Programm das **Ausführungsstadium** des Tasks in der Ansicht **Backup-Pläne und Tasks** an. Wenn der Task endet, wird im Fenster **Task-Information** das finale Stadium der Task-Ausführung angezeigt.

8.2.1 Auswahl des Archivs

So spezifizieren Sie ein zu exportierendes Archiv

1. Tragen Sie den vollständigen Pfad zum Archiv-Speicherort in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum (S. 115).
2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die sich in jedem von Ihnen gewählten Speicherort befinden.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder

modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

8.2.2 Auswahl der Backups

So wählen Sie ein zu exportierendes Backup aus

1. Aktivieren Sie oben im Fenster das bzw. die entsprechende(n) Kontrollkästchen.

   Um sicherzugehen, dass Sie das richtige Backup ausgewählt haben, klicken Sie auf das Backup; die untere Tabelle zeigt die in diesem Backup enthaltenen Volumes an.

   Um mehr Informationen über ein Volume zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen Sie im Kontextmenü **Informationen**.

2. Klicken Sie auf **OK**.

8.2.3 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für einen Zugriff auf den Ort notwendig sind, an dem das Quellarchiv oder das Backup gespeichert ist.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:

   - **Aktuelle Anmeldedaten verwenden**

     Die Software greift auf den Speicherort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.

   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:

     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.2.4 Speicherziel wählen

Spezifizieren Sie das Ziel, wohin das exportierte Objekt gespeichert werden soll. Backups dürfen nicht in dasselbe Archiv exportiert werden.

1. Exportziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel im Verzeichnisbaum aus.

- Um Daten in ein zentrales, nicht verwaltetes Depot zu exportieren, erweitern Sie die Gruppe **Zentrale Depots** und wählen dort ein Depot.
- Um Daten in ein persönliches Depot zu exportieren, erweitern Sie die Gruppe **Persönliche Depots** und wählen dort ein Depot.
- Um Daten in einen lokalen Ordner auf der Maschine zu exportieren, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.
- Um Daten zu einer Netzwerkfreigabe zu exportieren, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

  ***Hinweis für Linux-Benutzer**: Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Punkt wie z.B. /mnt/share angeschlossen ist, wählen Sie diesen Mount-Punkt statt der Netzwerkfreigabe aus.*

- Zum Datenexport auf einen **FTP**- oder **SFTP**-Server tragen Sie Server-Namen oder -Adresse folgendermaßen in das Feld **Pfad** ein:

  ftp://ftp-server:port-nummer oder **sftp://sftp-server:port-nummer**

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

  Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.

- Um Daten auf ein lokal angeschlossenes Bandgerät zu exportieren, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät. Bandgeräte sind in Acronis Backup Advanced verfügbar. In Acronis Backup sind Bandgeräte nur dann verfügbar, wenn Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgeräte.

2. Archiv-Tabelle verwenden

Die rechte Tabelle zeigt für jeden im Baum gewählten Speicherort die Namen der dort enthaltenen Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern.

Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort.
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt.
- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort.

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

8.2.5 Anmeldedaten für das Ziel

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das resultierende Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Aktuelle Anmeldedaten verwenden**

     Die Software greift auf den Zielort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.
   - **Folgende Anmeldedaten verwenden**

     Die Software greift auf den Zielort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Tasks keine Zugriffserlaubnis für den Zielort hat.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.3 Ein Image mounten

Indem Sie die Volumes eines Laufwerk-Backups (Images) mounten, können Sie auf diese Volumes so zugreifen, als wären es physikalische Laufwerke. Wenn mehrere Volumes im selben Backup enthalten sind, dann können Sie diese in einer einzigen Mount-Aktion gleichzeitig anschließen. Die Mount-Aktion ist verfügbar, wenn die Konsole mit einer verwalteten, unter Windows oder Linux laufenden Maschine verbunden ist.

Ein Anschließen der Partitionen im 'Lese/Schreib'-Modus erlaubt Ihnen, den Backup-Inhalt zu modifizieren, d.h. Dateien und Ordner zu speichern, zu verschieben, zu erstellen oder zu löschen und aus einer Datei bestehende, ausführbare Programme zu starten. Die Software erstellt in diesem Modus ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Beachten Sie, dass keine der nachfolgenden Backups diese Änderungen enthalten werden.

Sie können Volumes mounten, falls das Laufwerk-Backup in einem lokalen Ordner (ausgenommen optische Medien), in der Acronis Secure Zone oder auf einer Netzwerkfreigabe gespeichert vorliegt.

Einsatzszenarien

- **Freigeben**: gemountete Images können für Benutzer des Netzwerkes einfach freigegeben werden.

- **Notlösung zur Datenbankwiederherstellung**: mounten Sie ein Image, das eine SQL-Datenbank von einer kürzlich ausgefallenen Maschine enthält. Auf diese Weise erhalten Sie Zugriff auf die Datenbank, bis die ausgefallene Maschine wiederhergestellt ist.
- **Offline Virus-Bereinigung**: wenn eine Maschine befallen ist, fährt der Administrator diese herunter, startet mit einem bootfähigen Medium und erstellt ein Image. Danach mountet der Administrator dieses Image im 'Lese/Schreib'-Modus, scannt und bereinigt es mit einem Antivirus-Programm und stellt schließlich die Maschine wieder her.
- **Fehlerüberprüfung**: Wenn eine Wiederherstellung durch einen Laufwerksfehler fehlschlägt, mounten Sie das Image im 'Lese/Schreib'-Modus. Überprüfen Sie dann das gemountete Laufwerk mit dem Befehl **chkdsk /r**.

Führen Sie folgende Schritte aus, um ein Image zu mounten.

Quelle

Archiv (S. 182)

Spezifizieren Sie den Pfad zum Speicherort des Archivs und wählen Sie die in diesem enthaltenen Laufwerk-Backups.

Backup (S. 183)

Wählen Sie das Backup.

Anmeldedaten (S. 183)

[Optional] Geben Sie die Anmeldeinformationen für den Speicherort des Archivs an.

Mount-Einstellungen

Volumes (S. 183)

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Mount-Einstellungen für jedes Laufwerk: Weisen Sie einen Laufwerksbuchstaben zu oder geben Sie den Mount-Punkt an, entscheiden Sie sich dann für den Lese-/Schreib- oder Nur-Lese-Zugriffsmodus.

Nachdem Sie alle benötigten Schritte abgeschlossen haben, klicken Sie auf **OK**, um die Partitionen zu mounten.

8.3.1 Auswahl des Archivs

So wählen Sie ein Archiv aus

1. Geben Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort aus dem Verzeichnisbaum:
   - Sollte das Archiv in einem persönlichen Depot gespeichert sein, welches sich in einem lokalen Ordner, in der Acronis Secure Zone oder einer Netzwerkfreigabe befindet, dann erweitern Sie die Gruppe **Persönlich** und klicken Sie auf das benötigte Depot.
   - Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen Sie das gewünschte Verzeichnis.

     Die Möglichkeit zum Mounten ist nicht verfügbar, falls das Archiv auf optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) gespeichert ist.
   - Falls das Archiv auf einer Netzwerkfreigabe gespeichert ist, dann erweitern Sie die Gruppe **Netzwerkordner**, wählen Sie die gewünschte Netzwerk-Maschine und klicken Sie dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

8.3.2 Auswahl der Backups

So wählen Sie ein Backup aus:

1. Bestimmen Sie eines der Backups anhand seines Zeitstempels.
2. Die untere Tabelle zeigt zur Unterstützung bei der Wahl des richtigen Backups die in diesem Backup enthaltenen Partitionen an.

   Um mehr Informationen über ein Laufwerk zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen im Kontextmenü **Informationen**.
3. Klicken Sie auf **OK**.

8.3.3 Anmeldedaten

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Aktuelle Anmeldedaten verwenden**

     Das Programm greift auf den Speicherort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das aktuelle Benutzerkonto keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.3.4 Auswahl der Partition

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Parameter zum Mounten für jedes der gewählten Laufwerke wie folgt:

1. Aktivieren Sie das Kontrollkästchen für jede Partition, die Sie mounten müssen.
2. Klicken Sie auf das gewählte Laufwerk, um die Parameter zum Mounten einzustellen.
   - **Zugriffsmodus** – bestimmen Sie den Modus, mit dem Sie das Laufwerk anschließen wollen:
     - **Nur Lesen** – ermöglicht Ihnen das Durchsuchen und Öffnen von Dateien innerhalb des Backups, ohne dass es zu irgendwelchen Änderungen kommen kann.

- **Lesen/Schreiben** – in diesem Modus geht das Programm davon aus, dass der Backup-Inhalt verändert wird, und erstellt ein inkrementelles Backup, um diese Veränderungen aufzunehmen.
- **Laufwerksbuchstabe zuweisen** (in Windows) – Acronis Backup wird dem angeschlossenen Laufwerk einen freien Laufwerksbuchstaben zuweisen. Wählen Sie sofern benötigt aus dem Listenfeld einen anderen Laufwerksbuchstaben.
- **Mount-Punkt** (in Linux) – spezifiziert das Verzeichnis, wo Sie die Partition gemountet haben wollen.

3. Sollten mehrere Partitionen zum Anschließen ausgewählt sein, so klicken Sie auf jedes Laufwerk, um wie im vorherigen Schritt beschrieben die Parameter zum Mounten einzustellen.
4. Klicken Sie auf **OK**.

8.3.5 Gemountete Images verwalten

Sobald eine Partition angeschlossen wurde, können Sie im Backup enthaltene Dateien und Ordner mit einem Datei-Manager durchsuchen und gewünschte Dateien zu einem beliebigen Ziel kopieren. Sie müssen daher keine vollständige Wiederherstellungsprozedur durchführen, wenn Sie nur einige Dateien und Ordner aus einem Partitions-Backup entnehmen müssen.

Images durchsuchen

Über das Durchsuchen von angeschlossenen Partitionen können Sie den Laufwerksinhalt einsehen und auch modifizieren (sofern im Lese-/Schreib-Modus gemountet).

Um eine angeschlossene Partition zu durchsuchen, wählen Sie das Laufwerk in der Tabelle aus und klicken auf **Durchsuchen**. Darauf öffnet sich das Fenster des Standard-Datei-Managers und erlaubt Ihnen so, den Inhalt des gemounteten Laufwerkes zu untersuchen.

Abbild abschalten

Ein gemountetes Laufwerk im System zu belassen, benötigt einiges an System-Ressourcen. Es ist daher empfehlenswert, dass Sie die Laufwerke, nachdem alle notwendigen Aktionen abgeschlossen wurden, wieder abschalten. Ein Laufwerk bleibt bis zum nächsten Neustart des Betriebssystems gemountet, wenn Sie es nicht manuell abschalten.

Um ein Image abzuschalten, wählen Sie es in der Tabelle aus und klicken dann auf **Abschalten**.

Um alle gemounteten Laufwerke abzuschalten, klicken Sie auf **Alle abschalten**.

8.4 In Depots verfügbare Aktionen

Durch die Verwendung von Depots haben Sie einen einfachen Zugriff auf Archive und Backups und können Sie Archivverwaltungsaktionen ausführen.

So führen Sie Aktionen mit Archiven und Backups aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot aus, dessen Archive Sie verwalten wollen.
2. Wählen Sie in der Ansicht 'Depot' die Registerlasche **Archiv-Anzeige**. Diese Registerlasche zeigt alle in dem gewählten Depot gespeicherten Archive an.
3. Wie Sie fortfahren ist beschrieben unter:
   - Aktionen mit Archiven (S. 185)
   - Aktionen mit Backups (S. 185)

8.4.1 Aktionen mit Archiven

So führen Sie Aktionen mit einem Archiv aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot, welches die Archive enthält.
2. Wählen Sie in der Registerlasche **Archiv-Anzeige** dieses Depots das gewünschte Archiv. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.
3. Führen Sie Aktionen aus, indem Sie auf die entsprechenden Schaltflächen der Symbolleiste klicken. Sie können auf diese Aktionen auch über das Hauptmenüelement **'[Archivname]' Aktionen** zugreifen.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Archiven, die in einem Depot gespeichert sind.

Aktion	Lösung
Ein Archiv validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung** (S. 172) mit dem bereits als Quelle vorausgewählten Archiv. Die Validierung eines Archivs überprüft die Gültigkeit aller Backups im Archiv.
Ein Archiv exportieren	Klicken Sie auf **Exportieren**. Darauf öffnet sich die Seite **Export** (S. 176) mit dem vorausgewählten Archiv als Quelle. Beim Export wird ein Duplikat des Archivs einschließlich aller enthaltenen Backups am von Ihnen angegebenen Speicherort erstellt.
Ein einzelnes oder mehrere Archive löschen	1. Wählen Sie ein oder mehrere Archive, das/die sie löschen wollen. 2. Klicken Sie auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 187), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Archiv), bestätigen Sie danach die Löschaktion.
Alle Archive in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl in einem neuen Fenster, welches für jedes Archiv bzw. Backup Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig; bestätigen Sie dann die Löschaktion.

8.4.2 Aktionen mit Backups

So führen Sie beliebige Aktionen mit einem Backup aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot, welches die Archive enthält.
2. Wählen Sie in der Registerlasche **Archiv-Anzeige** dieses Depots das gewünschte Archiv. Erweitern Sie dann das Archiv und klicken Sie auf das Backup, um es auszuwählen. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.
3. Führen Sie Aktionen aus, indem Sie auf die entsprechenden Schaltflächen der Symbolleiste klicken. Sie können auf diese Aktionen auch über das Hauptmenüelement **'[Backup-Name]' Aktionen** zugreifen.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Backups.

Aufgabe	Lösung
Backup-Inhalte in einem separaten Fenster einsehen	Klicken Sie auf **Inhalt anzeigen**. Überprüfen Sie im Fenster **Backup-Inhalt** die entsprechend angezeigten Daten.
Recovery	Klicken Sie auf **Recovery**. Sie gelangen zur Seite **Daten wiederherstellen** (S. 112), mit dem bereits als Quelle vorausgewählten Backup.
Ein Laufwerk-/Volume-Backup zu einer virtuellen Maschine konvertieren	Klicken Sie mit der rechten Maustaste auf das Laufwerk-Backup und wählen Sie **Zu VM konvertieren**. Sie gelangen zur Seite **Daten wiederherstellen** (S. 112), mit dem bereits als Quelle vorausgewählten Backup. Wählen Sie Zielort sowie Typ der neuen virtuellen Maschine und fahren Sie dann so wie bei einer regulären Laufwerk- bzw. Volume-Wiederherstellung fort.
Ein Backup validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung** (S. 172), mit dem bereits als Quelle vorausgewählten Backup. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien eines Backups an einen virtuellen Zielort. Die Validierung eines Laufwerk-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist.
Ein Backup exportieren	Klicken Sie auf **Exportieren**. Darauf öffnet sich die Seite **Exportieren** (S. 176) mit dem vorausgewählten Backup als Quelle. Beim Exportieren wird ein neues Archiv mit einer unabhängigen Kopie des Backups an dem von Ihnen angegebenen Speicherort erstellt.
Ein Backup zu einem Voll-Backup konvertieren	Klicken Sie auf **Zu Voll-Backup konvertieren**, um ein inkrementelles oder differentielles Backup durch ein Voll-Backup zu ersetzen, das dem gleichen Backup-Zeitpunkt entspricht. Zu weiteren Informationen siehe den Abschnitt 'Ein Backup zu einem Voll-Backup konvertieren (S. 186)'.
Ein einzelnes oder mehrere Backups löschen	Wählen Sie das gewünschte Backup und klicken Sie dann auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 187), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Backup); bestätigen Sie danach die Löschaktion.
Alle Archive und Backups in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 187), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig; bestätigen Sie dann die Löschaktion.

8.4.3 Ein Backup zu einem Voll-Backup konvertieren

Wenn in einem Archiv die Kette inkrementeller Backups ziemlich lang wird, können Sie die Zuverlässigkeit Ihres Archivs erhöhen, indem Sie ein inkrementelles Backup in ein Voll-Backup

konvertieren. Sie können auf Wunsch auch ein differentielles Backup konvertieren, falls es auf diesem beruhende inkrementelle Backups gibt.

Während der Konvertierung wird das gewählte inkrementelle oder differentielle Backup durch ein Voll-Backup ersetzt, das demselben Backup-Zeitpunkt entspricht. Die anderen, vorhergehenden Backups in der Kette werden nicht verändert. Alle nachfolgenden inkrementellen und differentiellen Backups werden bis zum nächsten Voll-Backup ebenfalls aktualisiert. Die neuen Backup-Versionen werden zuerst erstellt und erst danach werden die älteren gelöscht. Der Speicherort muss daher über ausreichend Speicherplatz verfügen, um vorübergehend die alten und neuen Versionen aufnehmen zu können.

Beispiel

Sie haben folgende Backup-Kette in Ihrem Archiv:

```
F1 I2 I3 I4 D5 I6 I7 I8 F9 I10 I11 D12 F13
```

Dabei steht **F** für Voll-Backup (Full), **I** für inkrementell und **D** für differentiell.

Sie konvertieren das **I4**-Backup zu einem Voll-Backup. Die Backups **I4, D5, I6, I7, I8** werden aktualisiert, während **I10 I11 D12** unverändert bleiben, da sie auf **F9** basieren.

Tipps zur Verwendung

Die Konvertierung erstellt keine Kopie eines Backups. Um eine selbstständige Kopie eines Backups auf einem Flash-Laufwerk (USB-Stick) oder Wechselmedium zu erhalten, verwenden Sie die Aktion 'Exportieren (S. 176)'.

Beim Mounten eines Images (S. 181) im 'Lese/Schreib'-Modus erstellt die Software ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Die nachfolgenden Backups werden diese Änderungen nicht enthalten. Falls Sie normalerweise eines der nachfolgenden Backups zu 'vollständig' konvertieren, tauchen keine dieser Änderungen im resultierenden Voll-Backup auf.

Beschränkungen

Für folgende Backups ist keine Konvertierung erlaubt:

- Backups, die auf Bändern, auf CDs/DVDs oder im Acronis Cloud Storage gespeichert sind.
- Backups, die vereinfachte Namen (S. 61) haben.
- Backups von Microsoft Exchange-Server-Daten.

8.4.4 Archive und Backups löschen

Das Fenster **Backups löschen** zeigt dieselbe Registerlasche wie die Ansicht „Depots“, jedoch mit Kontrollkästchen für jedes Archiv und Backup. Das von Ihnen zum Löschen gewählte Archiv bzw. Backup ist entsprechend markiert. Überprüfen Sie das von Ihnen zum Löschen gewählte Archiv bzw. Backup. Wenn Sie noch weitere Archive und Backups löschen müssen, aktivieren Sie die entsprechenden Kontrollkästchen, klicken dann auf **Ausgewählte löschen** und bestätigen die Löschaktion.

Was passiert, wenn ich ein Backup lösche, das als Basis für ein inkrementelles oder differentielles Backup dient?

Das Programm konsolidiert die beiden Backups, um die Archiv-Konsistenz zu wahren. Ein Beispiel: Sie löschen ein Voll-Backup, behalten aber das nächste inkrementelle. Die Backups werden zu einem

einzelnen Voll-Backup kombiniert, welches den Zeitstempel des inkrementellen Backups erhält. Wenn Sie ein inkrementelles oder differentielles Backup aus der Mitte einer Kette löschen, wird der resultierende Backup-Typ inkrementell.

Machen Sie sich bewusst, dass Konsolidierung nur eine Methode, aber keine Alternative zum Löschen ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im beibehaltenen inkrementellen oder differentiellen Backup fehlten.

Das Depot sollte genügend Speicherplatz für während einer Konsolidierung erstellte temporäre Dateien haben. Aus einer Konsolidierung resultierende Backups sind immer maximal komprimiert.

9 Bootfähiges Medium

Bootfähiges Medium

Ein bootfähiges Medium ist ein physikalisches Medium (CD, DVD, USB-Stick oder andere Wechselmedien, die vom BIOS einer Maschine als Boot-Gerät unterstützt werden), das auf jeder PC-kompatiblen Maschine startet und es Ihnen ermöglicht, den Acronis Backup Agenten in einer Linux-basierte Umgebung oder unter Windows Preinstallation Environment (WinPE) auszuführen (also ohne die Hilfe eines bereits vorhandenen Betriebssystems). Bootfähige Medien werden am häufigsten verwendet, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- auf Daten zuzugreifen und zu sichern, die in einem beschädigten System überlebt haben
- ein Betriebssystem auf fabrikneue Computer zu verteilen
- Volumes vom Typ 'Basis' oder 'Dynamisch' auf fabrikneuen Geräten einzurichten
- Laufwerke, die ein nicht unterstütztes Dateisystem verwenden, mit einem Sektor-für-Sektor-Backup zu sichern
- Daten 'offline' zu sichern, die wegen einer Zugangsbeschränkung, einer Sperrung durch laufende Anwendungen oder wegen anderer Gründe nicht 'online' gesichert werden können.

Eine Maschine kann in die genannten Umgebungen entweder mit physikalischen Medien oder durch Netzwerk-Booten von einem Acronis PXE Server, von einem Windows Deployment Service (WDS) oder Remote Installation Service (RIS) gestartet werden. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiger Medien betrachtet werden. Sie können mit demselben Assistenten bootfähige Medien erstellen und den PXE Server oder WDS/RIS-Dienste konfigurieren.

Linux-basiertes bootfähiges Medium

Linux-basierte Medien enthalten einen bootfähigen Acronis Backup Agenten, der auf einem Linux-Kernel beruht. Der Agent kann auf jeder PC-kompatiblen Hardware booten und dort Aktionen ausführen, einschließlich auf fabrikneuer Hardware und Maschinen mit beschädigten oder nicht unterstützten Dateisystemen. Diese Aktionen können per Management Konsole konfiguriert und gesteuert werden – lokal oder per Remotesteuerung.

PE-basiertes bootfähiges Medium

PE-basierte bootfähige Medien enthalten ein funktionsreduziertes Windows, Windows Preinstallation Environment (WinPE) genannt, sowie ein Acronis Plug-in für WinPE; dabei handelt es sich um eine Modifikation des Acronis Backup Agenten, damit dieser unter WinPE laufen kann.

WinPE hat sich gerade bei großen IT-Umgebungen mit unterschiedlicher Hardware als sehr praktische bootfähige Lösung erwiesen.

Vorteile:

- Die Verwendung von Acronis Backup in WinPE bietet mehr Funktionalität als die Verwendung Linux-basierter bootfähiger Medien. Indem Sie Ihre PC-kompatible Hardware mit WinPE booten, können Sie nicht nur den Acronis Backup Agenten verwenden, sondern auch PE-Befehle, Skripte und andere Plug-ins, die Sie in WinPE eingebunden haben.

- Bootfähige Medien auf PE-Basis helfen, Linux-bezogene Probleme zu umgehen, z.B. fehlende Unterstützung für RAID-Controller oder gewisse RAID-Level. Auf WinPE 2.x (und höher) basierende Medien ermöglichen es, benötigte Gerätetreiber dynamisch zu laden.

Beschränkungen:

- Bootfähige Medien, die auf WinPE vor Version 4.0 basieren, können keine Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.
- Wenn eine Maschine mit einem PE-basierten Boot-Medium gestartet wird, können Sie keine optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) als Backup-Ziel auswählen.

9.1 So erstellen Sie ein bootfähiges Medium

Acronis bietet Ihnen mit dem Acronis Bootable Media Builder ein spezielles Werkzeug zur Erstellung bootfähiger Medien.

Der Bootable Media Builder erfordert keine Lizenz, wenn er zusammen mit einem Agenten installiert wird. Um einen Media Builder auf einer Maschine ohne Agenten nutzen zu können, müssen Sie einen Lizenzschlüssel eingeben oder wenigstens eine Lizenz auf dem License Server verfügbar haben. Die Lizenz kann entweder verfügbar oder zugewiesen sein.

Um ein physikalisches Medium erzeugen zu können, muss die Maschine über einen CD-/DVD-Brenner verfügen oder ein Flash-Laufwerk (z.B. USB-Stick) anschließbar sein. Um PXE oder WDS/RIS konfigurieren zu können, muss die Maschine eine Netzverbindung haben. Der Bootable Media Builder kann außerdem das ISO-Image einer bootfähigen Disc erstellen, um dieses später auf ein leeres Medium zu brennen.

Nachfolgend finden Sie Anleitungen zur Erstellung bootfähiger Medien.

9.1.1 Linux-basiertes bootfähiges Medium

So erstellen Sie ein Linux-basiertes Boot-Medium

1. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigenständige Komponente.
2. Sollte der Agent für Windows oder der Agent für Linux auf der Maschine *nicht installiert* sein, dann spezifizieren einen Lizenzschlüssel oder einen License Server mit seinen Lizenzen. Die Lizenzen werden nicht zugewiesen oder neu zugewiesen. Sie helfen zu bestimmen, welche Funktionen für das erstellte Medium aktiviert werden sollen. Ohne Lizenz können Sie ein Medium erstellen, mit dem Sie nur Wiederherstellungen vom Cloud Storage durchführen können.

   Sollte der Agent für Windows oder der Agent für Linux auf der Maschine *doch installiert* sein, dann übernimmt das Medium dessen Funktionalität, einschließlich Universal Restore und Deduplizierung.
3. Wählen Sie den **Typ des bootfähigen Mediums: Standard (Linux-basiertes Medium)**.

   Bestimmen Sie, wie Volumes und Netzwerk-Ressourcen gehandhabt werden – den so genannten 'Stil' des Mediums:

   - Ein Medium mit Linux-typischer Volume-Behandlung stellt die Volumes beispielsweise als hda1 und sdb2 dar. Es versucht, MD-Geräte und logische Volumes (vom LVM verwaltet) vor Start einer Wiederherstellung zu rekonstruieren.
   - Ein Medium, das Volumes Windows-typisch behandelt, verwendet Laufwerksbuchstaben zur Darstellung von Volumes, beispielsweise C: und D:. Es bietet Zugriff auf dynamische Volumes (LDM verwaltet).

4. Folgen Sie den Assistentenschritten, um Folgendes zu spezifizieren:
   a. [Optional] Parameter für den Linux-Kernel. Trennen Sie mehrere Parameter per Leerzeichen.

      Um beispielsweise bei jedem Start des bootfähigen Agenten einen Anzeigemodus für das Medium auswählen zu können, geben Sie an: **vga=ask**

      Eine Liste der Parameter finden Sie unter 'Kernel-Parameter (S. 191)'.
   b. Die Acronis Bootable Components, die das bootfähige Medium später enthalten soll.

      Sie können 32-Bit- und/oder 64-Bit-Komponenten wählen. Die 32-Bit-Komponenten funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Komponenten, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

      Um das Medium auf verschiedenen Hardware-Typen verwenden zu können, wählen Sie beide Komponententypen. Wenn Sie dann eine Maschine mit dem resultierenden Medium booten, können Sie die 32-Bit- oder 64-Bit-Komponenten dann aus dem Boot-Menü auswählen.
   c. [Optional] Das Timeout-Intervall für das Boot-Menü, sowie die Komponente, die automatisch nach dem Zeitlimit gestartet wird.
      - Sofern nicht anders konfiguriert, wartet der Acronis Loader auf eine Auswahl, ob das Betriebssystem (sofern vorhanden) oder die Acronis-Komponente gestartet werden soll.
      - Wenn Sie z.B. **10 Sek.** für den bootfähigen Agenten einstellen, wird dieser 10 Sekunden nach Anzeige des Menüs starten. Dies ermöglicht den unbeaufsichtigten Betrieb vor Ort, wenn von einem PXE Server oder WDS/RIS gebootet wird.
   d. [Optional] Remote-Anmeldeeinstellungen:
      - Einzugebender Benutzername und Kennwort auf Konsolenseite bei Verbindung zum Agenten. Falls Sie diese Felder leer lassen, wird die Verbindung ohne die Angabe von Anmeldedaten aufgebaut.
   e. [Optional] Netzwerkeinstellungen (S. 193):
      - TCP/IP-Einstellungen, die dem Netzwerkadapter der Maschine zugewiesen werden.
   f. [Optional] Netzwerk-Port (S. 194):
      - Der TCP-Port, den der bootfähige Agent auf einkommende Verbindungen kontrolliert.
   g. Der zu erstellende Medientyp. Sie können:
      - CDs, DVDs oder andere bootfähige Medien erstellen (z.B. USB-Sticks), sofern das BIOS der Hardware das Booten von diesen Medien erlaubt
      - Ein ISO-Image des bootfähigen Mediums erstellen, um es später auf einen leeren Rohling zu brennen
      - Gewählte Komponenten auf den Acronis PXE Server hochladen
      - Die gewählten Komponenten auf einen WDS/RIS hochladen.
   h. [Optional] Windows System-Treiber zur Verwendung durch Acronis Universal Restore (S. 194). Dieses Fenster erscheint nur dann, wenn kein auf PXE oder WDS/RIS basierendes Medium ausgewählt wurde.
   i. Pfad zur ISO-Datei des Mediums oder Name oder IP-Adresse inklusive Anmeldedaten für den PXE-Server oder WDS/RIS.

9.1.1.1 Kernel-Parameter

In diesem Fenster können Sie einen oder mehrere Parameter des Linux-Kernel angeben. Diese werden automatisch wirksam, wenn das bootfähige Medium startet.

Typischerweise kommen diese Parameter zur Anwendung, wenn während der Arbeit mit bootfähigen Medien Probleme auftauchen. Normalerweise brauchen Sie in dieses Feld nichts einzutragen.

Sie können jeden dieser Parameter auch durch Drücken der Taste F11 im Boot-Menü angeben.

Parameter

Trennen Sie mehrere Parameter mit Leerzeichen.

acpi=off

Deaktiviert ACPI (Advanced Configuration and Power Interface). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

noapic

Deaktiviert APIC (Advanced Programmable Interrupt Controller). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

vga=ask

Erfragt den Grafikkartenmodus, der in der grafischen Benutzeroberfläche eines bootfähigen Mediums verwendet werden soll. Ist kein **vga**-Parameter angegeben, wird der Videomodus automatisch erkannt.

vga=*mode_number*

Spezifiziert den Grafikkartenmodus, der in der grafischen Benutzeroberfläche des bootfähigen Mediums verwendet werden soll. Die Modus-Nummer wird unter *mode_number* im Hexadezimalformat angegeben, z.B.: **vga=0x318**

Die Bildschirmauflösung und die Anzahl der Farben für eine Modus-Nummer können sich von Maschine zu Maschine unterscheiden. Es wird empfohlen, zunächst den Parameter **vga=ask** zu verwenden, um einen Wert für *mode_number* auszuwählen.

quiet

Deaktiviert die Anzeige von Pop-up-Meldungen während der Linux-Kernel geladen wird und startet danach die Management Konsole.

Dieser Parameter wird implizit bei der Erstellung von bootfähigen Medien spezifiziert; Sie können ihn jedoch im Boot-Menü entfernen.

Wenn der Parameter nicht angegeben ist, werden alle Meldungen beim Start angezeigt, gefolgt von einer Eingabeaufforderung. Geben Sie bei der Eingabeaufforderung folgenden Befehl ein, um die Management Konsole zu starten: **/bin/product**

nousb

Deaktiviert, dass das USB-Subsystem geladen wird.

nousb2

Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten, auch wenn dieser Parameter gesetzt ist. Mit dem Parameter können Sie manche USB-Laufwerke im USB 1.1-Modus verwenden, wenn sie im USB 2.0-Modus nicht arbeiten.

nodma

Deaktiviert den Speicherdirektzugriff (DMA) für alle IDE-Festplatten. Verhindert auf mancher Hardware ein Einfrieren des Kernels.

nofw

Deaktiviert die Unterstützung für die FireWire (IEEE1394)-Schnittstelle.

nopcmcia

Deaktiviert die Erkennung von PCMCIA-Hardware.

nomouse

Deaktiviert die Maus-Unterstützung.

module_name=**off**

Deaktiviert das Modul, dessen Name in *module_name* angeben ist. Um beispielsweise die Nutzung des SATA-Moduls zu deaktivieren, geben Sie folgenden Wert an: **sata_sis=off**

pci=bios

Erzwingt die Verwendung des PCI-BIOS statt direkt auf die Hardware-Geräte zuzugreifen. Dieser Parameter kann hilfreich sein, z.B. wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.

pci=nobios

Deaktiviert die Verwendung des PCI BIOS und erlaubt nur direkte Hardware-Zugriffsmethoden. Dieser Parameter kann z.B. hilfreich sein, wenn das bootfähige Medium nicht startet und dies wahrscheinlich durch das BIOS verursacht wird.

pci=biosirq

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Dieser Parameter kann hilfreich sein, wenn es dem Kernel nicht gelingt, Unterbrechungsanforderungen (IRQs) zuzuordnen oder den sekundären PCI-Bus auf dem Mainboard zu finden.

Auf einigen Maschinen funktionieren diese Aufrufe möglicherweise nicht richtig. Es kann unter Umständen aber der einzige Weg sein, die Interrupt Routing-Tabelle anzuzeigen.

9.1.1.2 Netzwerk-Einstellungen

Sie erhalten während der Erstellung bootfähiger Acronis-Medien die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Agenten verwendet werden. Die folgenden Parameter können vorkonfiguriert werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server

Sobald der bootfähige Agent auf einer Maschine gestartet ist, wird die Konfiguration auf die Netzwerkkarte (NIC) der Maschine angewendet. Wenn die Einstellungen nicht vorkonfiguriert wurden, benutzt der Agent eine DHCP-Autokonfiguration. Sie haben außerdem die Möglichkeit, die Netzwerkeinstellungen manuell vorzunehmen, sobald der bootfähige Agent auf der Maschine läuft.

Mehrfache Netzwerkverbindungen vorkonfigurieren

Sie können die TCP/IP-Einstellungen für bis zu zehn Netzwerkkarten vorkonfigurieren. Um sicherzustellen, dass jede Netzwerkkarte die passenden Einstellungen bekommt, sollten Sie das Medium auf dem Server erstellen, für den das Medium konfiguriert wird. Wenn Sie eine existierende NIC im Assistentenfenster anwählen, werden ihre Einstellungen zur Speicherung auf das Medium übernommen. Die MAC-Adresse jeder existierenden NIC wird ebenso auf dem Medium gespeichert.

Sie können die Einstellungen ändern, mit Ausnahme der MAC-Adresse; oder Einstellungen für nicht existierende NICs konfigurieren, falls das nötig ist.

Sobald der bootfähige Agent auf dem Server gestartet ist, fragt er die Liste der verfügbaren NICs ab. Diese Liste ist nach den Steckplätzen sortiert, die von den NICs belegt werden. An der Spitze stehen die, die dem Prozessor am nächsten liegen.

Der bootfähige Agent teilt jeder bekannten NIC die passenden Einstellungen zu, wobei die NICs anhand ihrer MAC-Adressen identifiziert werden. Nachdem die NICs mit bekannten MAC-Adressen konfiguriert wurden, bekommen die verbliebenen NICs (beginnend mit der untersten in der Liste) die Einstellungen zugewiesen, die Sie für unbekannte NICs vorkonfiguriert haben.

Sie können bootfähige Medien für jede beliebige Maschine konfigurieren – und nicht nur für die Maschine, auf der das Medium erstellt wurde. Um dies durchzuführen, konfigurieren Sie die NICs entsprechend ihrer Steckplatzreihenfolge in der betreffenden Maschine. NIC1 besetzt den zum Prozessor am nächsten liegenden Steckplatz, NIC2 wiederum den folgenden und so weiter. Wenn der bootfähige Agent auf der Maschine startet, wird er keine NICs mit bekannter MAC-Adresse finden und daher die NICs in der von Ihnen bestimmten Reihenfolge konfigurieren.

Beispiel

Der bootfähige Agent könnte einen der Netzwerkadapter zur Kommunikation mit der Management Konsole innerhalb des Fertigungsnetzwerkes nutzen. Für diese Verbindung könnte eine automatische Konfiguration durchgeführt werden. Größere Datenmengen für eine Wiederherstellung könnten über die zweite NIC übertragen werden, die in das dafür bestimmte Backup-Netzwerk mit Hilfe statischer TCP/IP-Einstellungen eingebunden ist.

9.1.1.3 Netzwerk-Port

Bei der Erstellung bootfähiger Medien finden Sie eine Option zur Vorkonfiguration des Netzwerk-Ports, auf dem der bootfähige Agent nach einkommenden Verbindungen horcht. Es besteht die Wahl zwischen:

- dem Standard-Port
- dem aktuell verwendeten Port
- dem neuen Port (geben Sie die Port-Nummer ein)

Sofern der Port nicht vorkonfiguriert wurde, verwendet der Agent die Standard-Port-Nummer (9876). Dieser Port wird außerdem auch als Standard von der Acronis Backup Management Console verwendet.

9.1.1.4 Treiber für Universal Restore

Während der Erstellung der bootfähigen Medien erhalten Sie eine Option, um Windows-Treiber dem Medium hinzuzufügen. Diese Treiber werden von Universal Restore verwendet, wenn Windows auf einer Maschine mit abweichender Hardware wiederhergestellt wird (Prozessor, Mainboard oder Massenspeichergerät sind anders als im ursprünglich gesicherten System).

Sie können Universal Restore auch konfigurieren:

- um das Medium nach Treibern zu durchsuchen, die auf die Ziel-Hardware am besten passen
- um die Massenspeichertreiber einzubinden, die Sie ausdrücklich vom Medium aus spezifiziert haben. Dies ist notwendig, wenn die Ziel-Hardware einen spezifischen Massenspeicher-Controller für Festplatten und ähnliche Laufwerke verwendet (wie SCSI-, RAID- oder Fibre Channel-Adapter).

Weitere Informationen finden Sie im Abschnitt 'Acronis Universal Restore (S. 128)'.

Die Treiber werden im sichtbaren Treiber-Ordner auf dem bootfähigen Medium hinterlegt. Die Treiber werden nicht in den RAM der Ziel-Maschine geladen, daher muss das Medium während der Universal Restore-Aktion eingelegt bzw. verbunden bleiben.

Einem bootfähigen Medium können Sie Treiber hinzufügen, wenn Sie ein Wechselmedium (bzw. dessen ISO-Abbild) oder ein entfernbares Medium (z. B. einen USB-Stick) erstellen. Treiber können nicht auf einen PXE Server oder WDS/RIS hochgeladen werden.

Die Treiber können zur Liste nur in Gruppen hinzugefügt werden, indem die INF-Dateien oder Ordner hinzugefügt werden, die solche Dateien enthalten. Die Wahl einzelner Treiber aus den INF-Dateien ist nicht möglich, der Media Builder informiert Sie jedoch über den Inhalt der Dateien.

So fügen Sie Treiber hinzu:

1. Klicken Sie auf **Hinzufügen** und wählen Sie dann die INF-Datei oder den die INF-Dateien enthaltenden Ordner.
2. Wählen Sie die INF-Datei oder den Ordner aus.
3. Klicken Sie auf **OK**.

Die Treiber können aus der Liste nur in Gruppen, durch Löschen der INF-Dateien, entfernt werden.

So entfernen Sie Treiber:

1. Wählen Sie die INF-Datei aus.
2. Klicken Sie auf **Entfernen**.

9.1.2 WinPE-basierte bootfähige Medien

Der Bootable Media Builder ermöglicht drei Methoden, um Acronis Backup in WinPE einzubinden:

- Das Acronis-Plug-in einem existierenden PE-ISO-Abbild hinzufügen. Das ist praktisch, wenn Sie das Plug-in einem früher konfigurierten, in Verwendung befindlichen PE-ISO-Abbild hinzufügen müssen.
- Ein PE-ISO-Abbild mit dem Plug-in neu erstellen.
- Das Acronis-Plug-in einer WIM-Datei zur zukünftigen Verwendung hinzufügen (manuelle ISO-Erstellung, andere Tools dem Image hinzufügen, usw.).

Der Bootable Media Builder unterstützt WinPE-Distributionen, die auf folgenden Kerneln beruhen:

- Windows Vista (PE 2.0)
- Windows Vista SP1 und Windows Server 2008 (PE 2.1).
- Windows 7 (PE 3.0), mit oder ohne das 'Supplement for Windows 7 SP1' (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)

Bootable Media Builder unterstützt sowohl 32-Bit- wie auch 64-Bit-WinPE-Distributionen. Die 32-Bit-WinPE-Distributionen funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Distributionen, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

Auf WinPE 4 (und höher) basierende PE-Images benötigen ungefähr 1 GB an RAM, um arbeiten zu können.

9.1.2.1 Vorbereitung: WinPE 2.x und 3.x

Um PE 2.x oder 3.x-Images erstellen oder modifizieren zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (WAIK) installiert ist. Wenn Sie keine Maschine mit AIK haben, gehen Sie wie nachfolgend beschrieben vor.

So bereiten Sie eine Maschine mit AIK vor

1. Download und Installation des Windows Automated Installation Kit.

   Automated Installation Kit (AIK) für Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=de

   Automated Installation Kit (AIK) für Windows Vista SP1 und Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=de

   Automated Installation Kit (AIK) für Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=de

   Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):

   http://www.microsoft.com/de-de/download/details.aspx?id=5188

   Sie können die Systemanforderungen zur Installation finden, indem Sie den unteren Links folgen.
2. [Optional] Brennen Sie das WAIK auf DVD oder kopieren Sie es auf ein Flash-Laufwerk (USB-Stick).
3. Installieren Sie Microsoft .NET Framework von diesem Kit (NETFXx86 oder NETFXx64, abhängig von Ihrer Hardware).
4. Installieren Sie Microsoft Core XML (MSXML) 5.0 oder 6.0 Parser von diesem Kit.
5. Installieren Sie Windows AIK von diesem Kit.
6. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

Es ist empfehlenswert, dass Sie sich mit der dem Windows AIK beiliegenden Hilfe-Dokumentation vertraut machen. Um auf die Dokumentation zuzugreifen, wählen Sie **Microsoft Windows AIK -> Dokumentation** im Startmenü.

9.1.2.2 Vorbereitung: WinPE 4.0 und WinPE 5.0

Um Images von PE 4 oder PE 5 erstellen oder ändern zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Assessment and Deployment Kit (ADK) installiert ist. Wenn Sie keine Maschine mit ADK haben, gehen Sie wie nachfolgend beschrieben vor.

So bereiten Sie eine Maschine mit ADK vor

1. Laden Sie das Setup-Programm des von Assessment and Deployment Kits herunter.

   Assessment and Deployment Kit (ADK) für Windows 8 (PE 4.0):
   http://www.microsoft.com/de-de/download/details.aspx?id=30652 .

   Assessment and Deployment Kit (ADK) für Windows 8.1 (PE 5.0):
   http://www.microsoft.com/de-DE/download/details.aspx?id=39982 .

   Sie können die Systemanforderungen zur Installation finden, indem Sie den unteren Links folgen.
2. Installieren Sie das Assessment and Deployment Kit auf der Maschine.
3. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

9.1.2.3 Das Acronis Plug-in einem WinPE-Image hinzufügen

So fügen Sie das Acronis-Plug-in einem WinPE-ISO-Abbild hinzu:

1. Wenn Sie das Plug-in der existierenden WinPE-ISO-Datei hinzufügen, entpacken Sie alle Dateien Ihrer WinPE-ISO in einen separaten Laufwerksordner.
2. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigenständige Komponente.
3. Sollte der Agent für Windows auf der Maschine *nicht installiert* sein, dann spezifizieren einen Lizenzschlüssel oder einen License Server mit seinen Lizenzen. Die Lizenzen werden nicht zugewiesen oder neu zugewiesen. Sie helfen zu bestimmen, welche Funktionen für das erstellte Medium aktiviert werden sollen. Ohne Lizenz können Sie ein Medium erstellen, mit dem Sie nur Wiederherstellungen vom bzw. aus dem Cloud Storage durchführen können.

   Sollte der Agent für Windows auf der Maschine *doch installiert* sein, dann übernimmt das Medium dessen Funktionalität, einschließlich Universal Restore und Deduplizierung.
4. Wählen Sie den **Typ des bootfähigen Mediums: Windows PE**.

   Wenn Sie eine neue PE-ISO-Datei erstellen:
   - Wählen Sie den Befehl **WinPE automatisch erstellen**.
   - [Optional] Aktivieren Sie zur Erstellung eines 64-Bit-Boot-Mediums das Kontrollkästchen **x64-Medium erstellen** (sofern verfügbar). Sie benötigen ein 64-Bit-Medium, um eine Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.
   - Die Software führt das passende Skript aus und wechselt zum nächsten Fenster.

   So fügen Sie das Plug-in einem existierenden PE-ISO-Abbild hinzu:
   - Wählen Sie **WinPE-Dateien im von mir spezifizierten Ordner verwenden**.
   - Geben Sie den Pfad zum Ordner mit den WinPE-Dateien an.
5. [Optional] Wählen Sie, ob Remote-Verbindungen für eine per Boot-Medium gestartete Maschine (de)aktiviert werden sollen. Sind diese aktiviert, dann spezifizieren Sie den Benutzernamen und das Kennwort, welche auf Seiten der Konsole bei der Verbindung zum Agenten eingegeben werden sollen. Falls Sie diese Boxen leerlassen, wird die Verbindung deaktiviert.
6. Spezifizieren Sie die Netzwerkeinstellungen (S. 193) für den Netzwerkadapter der Maschine oder wählen Sie eine Autokonfiguration per DHCP.
7. [Optional] Spezifizieren Sie die Windows-Treiber, die Windows PE hinzugefügt werden sollen.

   Wenn Sie eine Maschine mit Windows PE booten, ermöglichen Ihnen diese Treiber, auf Geräte zuzugreifen, auf denen sich Ihre Backup-Archive befinden. Verwenden Sie 32-Bit-Treiber, sofern Sie eine 32-Bit-WinPE-Distribution verwenden – oder 64-Bit-Treiber, sofern Sie eine 64-Bit-WinPE-Distribution einsetzen.

   Sie können auf die hinzugefügten Treiber auch verweisen, wenn Sie Universal Restore konfigurieren. Fügen Sie zur Verwendung von Universal Restore entweder 32-Bit- oder 64-Bit-Treiber hinzu; abhängig davon, ob Sie ein 32-Bit- oder 64-Bit-Betriebssystemvariante von Windows wiederherstellen wollen.

   So fügen Sie Treiber hinzu:
   - Klicken Sie auf **Hinzufügen** und geben Sie den Pfad zur notwendigen *. inf-Datei für einen entsprechenden SCSI-, RAID- oder SATA-Controller, einen Netzwerkadapter, ein Bandlaufwerk oder andere Geräte an.
   - Wiederholen Sie dieses Prozedur für jeden Treiber, den Sie in das resultierende WinPE-Boot-Medium aufnehmen wollen.
8. Wählen Sie, ob Sie ein ISO- oder WIM-Image erstellen wollen oder das Medium auf einen Server (Acronis PXE Server, WDS oder RIS) hochgeladen werden soll.

9. Geben Sie den vollen Pfad einschließlich Dateiname zur resultierenden Image-Datei an – oder spezifizieren Sie den Server inklusive Benutzername und Kennwort für den Zugriff.
10. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie auf **Fertig stellen**.
11. Brennen Sie die ISO-Datei auf CD oder DVD (durch das Brennprogramm eines Drittherstellers) oder kopieren Sie die Daten auf ein Flash-Laufwerk wie einen USB-Stick (Daten und Flash-Laufwerk müssen zum Booten separat angepasst werden).

Sobald eine Maschine mit WinPE gebootet wird, startet Acronis Backup automatisch.

So erstellen Sie ein PE-Abbild (ISO-Datei) von einer resultierenden WIM-Datei:

- Ersetzen Sie die vorgegebene boot.wim-Datei im Windows PE-Ordner mit der neu erstellten WIM-Datei. Für das genannte Beispiel geben Sie ein:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- verwenden Sie das Tool **Oscdimg**. Für das genannte Beispiel geben Sie ein:

```
oscdimg -n –bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
c:\winpe_x86\winpe_x86.iso
```

Weitere Informationen zur Anpassung von Windows PE finden Sie im Windows PE-Benutzerhandbuch (Winpe.chm).

9.2 Verbinde mit einer Maschine, die von einem Medium gebootet wurde

Sobald eine Maschine von einem bootfähigen Medium gestartet ist, erscheint ein Konsolenfenster mit den IP-Adressen, die per DHCP oder als manuell vorkonfigurierte Werte zugewiesen wurden.

Netzwerkeinstellungen konfigurieren

Klicken Sie zum Ändern der Netzwerkeinstellungen für eine aktuelle Sitzung im Startfenster auf **Netzwerk konfigurieren**. Das erscheinende Fenster **Netzwerkeinstellungen** ermöglicht Ihnen, die Netzwerkeinstellungen für jede Netzwerkkarte (NIC) auf der Maschine zu konfigurieren.

Während einer Sitzung durchgeführte Änderungen gehen nach dem Neustart der Maschine verloren.

VLANs hinzufügen

Sie können im Fenster **Netzwerkeinstellungen** VLANs (Virtual Local Area Networks, virtuelle lokale Netzwerke) hinzufügen. Verwenden Sie diese Funktionalität, falls Sie auf einen Backup-Speicherort zugreifen müssen, der sich in einem spezifischen VLAN befindet.

VLANs werden hauptsächlich dazu verwendet, um lokale Netzwerke (LANs) in logische Teilnetze zu segmentieren. Eine Netzwerkkarte (NIC), die mit einem *Zugriffs*-Port des Switches verbunden ist, kann immer auf das in der Port-Konfiguration spezifizierte VLAN zugreifen. Eine Netzwerkkarte (NIC), die mit einem *Trunk*-Port des Switches verbunden ist, kann nur dann auf die in der Port-Konfiguration erlaubten VLANs zugreifen, wenn Sie die VLANs in den Netzwerkeinstellungen spezifizieren.

So ermöglichen Sie den Zugriff auf ein VLAN über einen Trunk-Port

1. Klicken Sie auf **VLAN hinzufügen**.
2. Wählen Sie die Netzwerkkarte aus, die Zugriff auf dasjenige lokale Netzwerk bereitstellt, welches das benötigte VLAN enthält.
3. Spezifizieren Sie den VLAN-Bezeichner (Identifier).

Nachdem Sie auf **OK** geklickt haben, erscheint in der Liste der Netzwerkadapter ein neuer Eintrag.

Sollten Sie ein VLAN entfernen wollen, dann klicken Sie auf den erforderlichen VLAN-Eintrag – und anschließend auf **VLAN entfernen**.

Lokale Verbindung

Um direkt auf einer Maschine arbeiten zu können, die mit einem bootfähigen Medium gestartet wurde, müssen Sie im Startfenster auf **Diese Maschine lokal verwalten** klicken.

Remote-Verbindung

Um eine Management Konsole mit einer Remote-Maschine zu verbinden, die mit einem bootfähigen Medium gestartet wurde, müssen Sie im Konsolen-Menü die Befehle **Verbinden –> Remote-Maschine verwalten** wählen. Spezifizieren Sie anschließend eine der IP-Adressen der Maschine. Geben Sie Anmeldedaten (Benutzername, Kennwort) ein, falls diese bei Erstellung des Bootmediums konfiguriert wurden.

9.3 Mit bootfähigen Medien arbeiten

Die Arbeitsweise mit einer Maschine, die per bootfähigem Medium gestartet wurde, ist sehr ähnlich zu den Backup- und Recovery-Aktionen unter dem sonst üblichen Betriebssystem. Der Unterschied ist folgender:

1. Unter einem Windows-typischen bootfähigen Medium hat ein Volume denselben Laufwerksbuchstaben wie unter Windows. Volumes, die unter Windows keine Laufwerksbuchstaben haben (wie etwa das Volume **System-reserviert**) bekommen freie Laufwerksbuchstaben in der Reihenfolge ihres Vorkommens auf den Laufwerken zugewiesen.

   Sollte das bootfähige Medium kein Windows auf der Maschine erkennen können oder mehrere Windows-Versionen erkennen, dann wird allen Volumes (einschließlich derer ohne Laufwerksbuchstaben) in der Reihenfolge ihres Vorkommens auf den Laufwerken ein Buchstabe zugewiesen. Auf diese Art können die Laufwerksbuchstaben dann von denen unter Windows vorliegenden abweichen. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem bootfähigen Medium dem Laufwerk E: entsprechen, welches Windows verwendet.

   Achtung! Um auf der sicheren Seite zu sein, ist es ratsam, den jeweils verwendeten Volumes eindeutige Namen zuzuweisen.

2. Ein Linux-typisches bootfähiges Medium zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).
3. Mit einem bootfähigen Medium erstellte Backups werden mit einer vereinfachten Dateibenennung (S. 61) gekennzeichnet. Backups erhalten nur dann Standardnamen, wenn diese einem bereits existierenden Archiv, welches einen Standarddateinamen verwendet, hinzugefügt werden – oder falls der Zielort keine vereinfachte Dateibenennung unterstützt.
4. Ein bootfähiges Medium im Stil 'Linux-typisch' kann keine Backups auf ein NTFS-formatiertes Volume schreiben. Wechseln Sie zum Stil 'Windows-typisch', wenn Sie diese Funktion benötigen.
5. Sie können den Arbeitsstil des bootfähigen Mediums zwischen Windows- und Linux-typisch umschalten, indem Sie **Extras** –> **Volume-Darstellung ändern** wählen.
6. Der Verzeichnisbaum **Navigation** ist in der Benutzeroberfläche des Mediums nicht vorhanden. Verwenden Sie den Menübefehl **Navigation**, um zwischen verschiedenen Ansichten umzuschalten.
7. Es können keine geplanten Tasks benutzt werden, da grundsätzlich keine Tasks erstellt werden können. Um eine Aktion zu wiederholen, konfigurieren Sie sie von Anfang an neu.

8. Der Speicherzeitraum für Ereignisse (Logs) ist auf die aktuelle Sitzung beschränkt. Sie können die gesamte Ereignisliste oder gefilterte Logs in eine Datei speichern.

9.3.1 Einen Anzeigemodus einstellen

Bei einer von einem bootfähigen Medium gestarten Maschine wird der Anzeigemodus basierend auf der Hardware-Konfiguration automatisch erkannt (Monitor- und Grafikkarten-Spezifikationen). Sollte aus irgendeinem Grund der Darstellungsmodus nicht korrekt erkannt werden, gehen Sie folgendermaßen vor:

1. Drücken Sie im Boot-Menü auf F11.
2. Geben Sie in die Eingabeaufforderung folgenden Befehl ein: **vga=ask**, fahren Sie dann mit dem Boot-Vorgang fort.
3. Wählen Sie aus der Liste der verfügbaren Darstellungsmodi den passenden durch Eingabe seiner Nummer (z.B. **318**), drücken Sie dann auf Enter.

Falls Sie diese Schritte nicht jedes Mal ausführen möchten, wenn Sie auf einer bestimmten Hardwarekonfiguration von einem Boot-Medium starten, erstellen Sie das Medium mit der entsprechenden Modus-Nummer (in unserem Beispiel: **vga=0x318**) im Fenster **Kernel-Parameter** (weitere Informationen finden Sie im Abschnitt Bootable Media Builder (S. 190)).

9.3.2 iSCSI- und NDAS-Geräte konfigurieren

Dieser Abschnitt beschreibt, wie iSCSI (Internet Small Computer System Interface)- und NDAS (Network Direct Attached Storage)-Geräte bei der Arbeit mit bootfähigen Medien konfiguriert werden.

Diese Geräte sind über eine Netzwerkschnittstelle mit der Maschine verbunden und werden angezeigt, als wären sie lokal angeschlossene Geräte. Im Netzwerk werden iSCSI-Geräte über ihre IP-Adresse und NDAS-Geräte über ihre Geräte-ID identifiziert.

iSCSI-Geräte werden manchmal auch als iSCSI-Target bezeichnet. Eine Hard- oder Software-Komponente, die das Zusammenspiel von Maschine und iSCSI-Target ermöglicht, wird als iSCSI-Initiator bezeichnet. Der Name des iSCSI-Initiators wird üblicherweise durch den Administrator des Servers bestimmt, der das Gerät hostet.

So fügen Sie ein iSCSI-Gerät hinzu

1. Führen sie in einem (Linux- oder PE-basierten) Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren** (in einem Linux-basierten Medium) bzw. auf **iSCSI-Setup ausführen** (in einem PE-basierten Medium).
3. Geben Sie vom Host des iSCSI-Gerät die IP-Adresse und den Port an und zudem den Namen des iSCSI-Initiators.
4. Benötigt der Host eine Authentifizierung, dann geben Sie Benutzernamen und Kennwort ein.
5. Klicken Sie auf **OK**.
6. Wählen Sie das iSCSI-Gerät aus der Liste und klicken Sie dann auf **Verbinden**.
7. Spezifizieren Sie bei Erscheinen einer Eingabeaufforderung Benutzernamen und Kennwort, um auf das iSCSI-Gerät zugreifen zu können.

So fügen Sie ein NDAS-Gerät hinzu

1. Führen sie in einem Linux-basierten Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren**.
3. Klicken Sie in **NDAS-Geräte** auf **Gerät hinzufügen**.

4. Geben Sie die 20-stellige Geräte-ID an.
5. Geben Sie den fünfstelligen Schreibschlüssel an, wenn Sie erlauben wollen, dass Daten auf das Gerät geschrieben werden. Ohne diesen Schlüssel wird das Gerät nur im 'Read-only'-Modus verfügbar sein.
6. Klicken Sie auf **OK**.

9.4 Liste verfügbarer Befehle und Werkzeuge in Linux-basierten bootfähigen Medien

Linux-basierte Boot-Medien enthalten folgende Kommandos und Befehlszeilen-Werkzeuge, die Sie bei Ausführung einer Eingabeaufforderung nutzen können. Zum Starten der Eingabeaufforderung drücken Sie Strg+Alt+F2, während Sie in der Management Konsole des bootfähigen Mediums sind.

Acronis Command-Line Utilities

- `acrocmd`
- `acronis`
- `asamba`
- `lash`

Linux-Befehle und Werkzeuge

`busybox`	`ifconfig`	`rm`
`cat`	`init`	`rmmod`
`cdrecord`	`insmod`	`route`
`chmod`	`iscsiadm`	`scp`
`chown`	`kill`	`scsi_id`
`chroot`	`kpartx`	`sed`
`cp`	`ln`	`sg_map26`
`dd`	`ls`	`sh`
`df`	`lspci`	`sleep`
`dmesg`	`lvm`	`ssh`
`dmraid`	`mdadm`	`sshd`
`e2fsck`	`mkdir`	`strace`
`e2label`	`mke2fs`	`swapoff`
`echo`	`mknod`	`swapon`
`egrep`	`mkswap`	`sysinfo`
`fdisk`	`more`	`tar`
`fsck`	`mount`	`tune2fs`
`fxload`	`mtx`	`udev`

gawk	**mv**	**udevinfo**
gpm	**pccardctl**	**udevstart**
grep	**ping**	**umount**
growisofs	**pktsetup**	**uuidgen**
grub	**poweroff**	**vconfig**
gunzip	**ps**	**vi**
halt	**raidautorun**	**zcat**
hexdump	**readcd**	
hotplug	**reboot**	

9.5 Acronis Startup Recovery Manager

Der Acronis Startup Recovery Manager ist eine Modifikation des bootfähigen Agenten (S. 296), befindet sich unter Windows auf der Systemfestplatte bzw. unter Linux auf der /boot-Partition und ist so konfiguriert, dass er durch Drücken von F11 während des Boot-Vorgangs gestartet wird. Dies bietet eine Alternative zum Start des bootfähigen Notfallwerkzeugs über ein separates Medium oder eine Netzwerkverbindung.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, booten Sie die Maschine neu und drücken die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…" erscheint. Darauf wird das Programm gestartet und Sie können die Wiederherstellung durchführen.

Sie können außerdem auch Backups mit dem Acronis Startup Recovery Manager erstellen, wenn sie unterwegs sind.

Auf Maschinen, die einen GRUB Boot-Loader installiert haben, wählen Sie den Acronis Startup Recovery Manager aus dem Boot-Menü, statt F11 zu drücken.

Aktivieren

Die Aktivierung schaltet die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager…" ein (sofern Sie keinen GRUB Boot-Loader haben) oder fügt den Menü-Eintrag „Acronis Startup Recovery Manager" zum Menü von GRUB hinzu (sofern Sie GRUB haben).

Auf der Systemfestplatte (bzw. der /boot-Partition unter Linux) sollten mindestens 100 MB freier Speicherplatz verfügbar sein, um den Acronis Startup Recovery Manager zu aktivieren.

Die Aktivierung des Acronis Startup Recovery Manager überschreibt den Master Boot Record (MBR) mit seinem eigenen Boot-Code, außer Sie verwenden den GRUB Boot-Loader und dieser ist im MBR installiert. Daher müssen Sie möglicherweise auch die Boot-Loader von Drittherstellern reaktivieren, wenn diese installiert sind.

Wenn Sie unter Linux einen anderen Boot-Loader als GRUB verwenden (etwa LILO), sollten Sie erwägen, diesen statt in den MBR in den Boot-Record einer Linux-root- oder Boot-Partition zu installieren, bevor Sie den Acronis Startup Recovery Manager aktivieren. Konfigurieren Sie anderenfalls den Boot-Loader manuell nach der Aktivierung.

Nicht aktivieren

Deaktiviert die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ (oder den Menü-Eintrag in GRUB). Falls der Acronis Startup Recovery Manager nicht aktiviert ist, müssen Sie zur Wiederherstellung eines nicht mehr bootfähigen Systems Folgendes tun:

- Booten Sie die Maschine mit Hilfe eines separaten, bootfähigen Notfallmediums.
- Verwenden Sie einen Netzwerk-Boot von einem Acronis PXE Server oder Microsoft Remote Installation Services (RIS).

10 Laufwerksverwaltung

Acronis Disk Director Lite ist ein Tool, das dazu dient, die Laufwerks-/Volume-Konfiguration einer Maschine für Wiederherstellungen von Volume-Images vorzubereiten, die per Acronis Backup-Software erstellt wurden.

Nachdem ein Laufwerk gesichert und sein Image an einem sicheren Speicherplatz hinterlegt wurde, kann es vorkommen, dass sich die Laufwerkskonfiguration der Maschine durch Austausch einer Festplatte oder durch Hardware-Verlust ändert. In diesem Fall hat der Benutzer durch die Hilfe des Acronis Disk Director Lite die Möglichkeit, die notwendige Laufwerkskonfiguration wieder so zu erstellen, dass das Laufwerksabbild exakt 'wie es war' wiederhergestellt werden kann (oder mit jeder Abweichung der Laufwerk-/Volume-Struktur, die der Benutzer für notwendig hält).

Alle Laufwerk- und Volume-Aktionen bergen ein gewisses Risiko von Datenverlust. Aktionen auf System- oder Daten-Volumes müssen sehr sorgfältig ausgeführt werden, um mögliche Probleme mit dem Boot-Ablauf oder Laufwerksdatenspeicher zu vermeiden.

Aktionen mit Laufwerken und Volumes benötigen eine gewisse Zeit – und Stromverlust, unbeabsichtigtes Ausschalten der Maschine oder versehentliches Drücken des Reset-Schalters während der Prozedur können zur Beschädigung des Volumes und Datenverlust führen.

Alle Aktionen mit den Volumes dynamischer Laufwerke in Windows XP und Windows 2000 setzen voraus, dass der Acronis Managed Machine Service unter einem Benutzerkonto mit Administrator-Rechten ausgeführt wird.

Treffen Sie alle notwendigen Vorsichtsmaßnahmen (S. 204), um einen möglichen Datenverlust zu vermeiden.

10.1 Unterstützte Dateisysteme

Der Acronis Disk Director Lite unterstützt die folgenden Dateisysteme:

- FAT 16/32
- NTFS

Wenn Sie mit einem Volume, das ein andere Dateisystem hat, eine Aktion durchzuführen müssen, dann verwenden Sie die Vollversion des Acronis Disk Director. Dieses Programm bietet noch mehr Tools und Utilities, um Festplatten und Volumes mit den folgenden Dateisystemen zu verwalten:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

10.2 Grundlegende Vorsichtsmaßnahmen

Treffen Sie alle notwendigen Vorsichtsmaßnahmen, um mögliche Schäden an der Laufwerks- bzw. Volume-Struktur oder Datenverlust abzuwenden und beachten Sie folgende grundsätzliche Regeln:

1. Erstellen Sie von Laufwerken, auf denen Volumes erstellt oder verwaltet werden, ein Backup. Indem Sie wichtige Daten auf ein anderes Laufwerk, eine Netzwerkfreigabe oder Wechselmedien sichern, können Sie – wohl wissend, dass Ihre Daten gut geschützt sind – beruhigt mit Ihren Laufwerken bzw. Volumes arbeiten.
2. Überprüfen Sie Ihre Festplatte, um sicherzustellen, dass sie voll funktionstüchtig ist und keine defekten Sektoren oder Dateisystemfehler enthält.
3. Führen Sie keine Laufwerks- bzw. Volume-Aktionen aus, während andere Programme mit Low-Level-Zugriff auf Laufwerke ausgeführt werden. Beenden Sie diese Programme bevor Sie Acronis Disk Director Lite ausführen.

Durch diese einfachen Vorsichtsmaßnahmen schützen Sie sich vor versehentlichem Datenverlust.

10.3 Acronis Disk Director Lite ausführen

Sie können Acronis Disk Director Lite unter Windows oder über ein bootfähiges Medium ausführen.

Beschränkungen

- Der Acronis Disk Director Lite ist unter bzw. für Windows 8/8.1 und für den Windows Server 2012/2012 R2 nicht verfügbar.
- Aktionen zur Laufwerksverwaltung funktionieren unter einem bootfähigen Medium möglicherweise nicht korrekt, falls auf der Maschine Speicherplätze (Storage Spaces) konfiguriert sind.

Acronis Disk Director Lite unter Windows ausführen

Wenn Sie die Acronis Backup Management Console starten und mit einer verwalteten Maschine verbinden, steht die Ansicht **Laufwerksverwaltung** im Zweig **Navigation** der Konsole zur Verfügung, von wo aus Sie den Acronis Disk Director Lite starten können.

Acronis Disk Director Lite von einem bootfähigen Medium ausführen

Sie können Acronis Disk Director Lite auf einer fabrikneuen, einer Nicht-Windows-Maschine oder einer, die nicht booten kann, ausführen. Um dies zu tun, booten Sie die Maschine von einem bootfähigen Medium (S. 296), das mit dem Acronis Bootable Media Builder erstellt wurde; starten die Management Konsole und klicken dann auf **Laufwerksverwaltung**.

10.4 Auswählen des Betriebssystems für die Datenträgerverwaltung

Auf einer Maschine mit zwei oder mehr Betriebssystemen hängt die Darstellung der Datenträger und Volumes davon ab, welches Betriebssystem gerade ausgeführt wird.

Ein Volume kann in verschiedenen Windows-Betriebssystemen auch unterschiedliche Buchstaben haben. Es kann z.B. sein, dass Volume „E:“ als „D:“ oder „L:“ angezeigt wird, wenn Sie ein anderes Windows-Betriebssystem booten, das auf derselben Maschine installiert ist. (Es ist aber auch möglich, dass dieses Volume unter allen auf der Maschine installierten Windows-Betriebssystemen als „E:“ angezeigt wird.)

Ein unter einem Windows-Betriebssystem erstellter dynamischer Datenträger wird in einem anderen Betriebssystem als **Fremder Datenträger** angesehen oder möglicherweise von diesem Betriebssystem gar nicht unterstützt.

Wenn Sie eine Aktion zur Datenträgerverwaltung mit einer solchen Maschine ausführen müssen, dann müssen Sie angeben, für welches Betriebssystem das Laufwerkslayout angezeigt und die Datenträgerverwaltungsaktion ausgeführt wird.

Der Name des aktuell ausgewählten Betriebssystems wird in der Symbolleiste der Konsole hinter **Das aktuelle Laufwerkslayout ist für:** angezeigt. Um ein anderes Betriebssystem auszuwählen, klicken Sie im Fenster **Auswahl des Betriebssystems** auf den Namen des Betriebssystems. Dieses Fenster wird unter den bootfähigen Medien angezeigt, nachdem Sie auf **Laufwerksverwaltung** geklickt haben. Das Laufwerkslayout wird so angezeigt, wie es dem ausgewählten Betriebssystem entspricht.

10.5 Ansicht „Laufwerksverwaltung"

Acronis Disk Director Lite wird über die **Laufwerksverwaltung**-Ansicht der Konsole kontrolliert.

Der oberste Bereich der Ansicht enthält eine Laufwerks- und Volume-Tabelle mit der Möglichkeit zur Sortierung, zur Anpassung der Spalten und verfügt über eine Symbolleiste. Die Tabelle präsentiert alle verfügbaren Laufwerke, zugewiesene Laufwerksbuchstaben und -bezeichnungen, Laufwerkstyp sowie -kapazität, freien und benutzten Speicherplatz, Dateisystem und Status eines jeden Laufwerks. Die Symbolleiste beinhaltet Icons zum Starten der Aktionen **Rückgängig**, **Wiederherstellen**und **Ausführen**, die sich auf ausstehende Aktionen (S. 220) beziehen.

Über den grafischen Bereich im unteren Teil der Ansicht werden alle Laufwerke und ihre Volumes noch einmal als Rechtecke visualisiert, inklusive ihrer Basisdaten (Bezeichnung, Laufwerksbuchstabe, Größe, Status, Typ und Dateisystem).

Beide Teile der Ansicht bilden zudem den verfügbaren nicht zugeordneten Speicherplatz ab, der zur Erstellung von Laufwerken verwendet werden kann.

Aktionen starten

Jede Aktion kann folgendermaßen gestartet werden:

- vom Kontextmenü der Laufwerke oder Festplatten (in der Tabelle und in der grafischen Ansicht)
- aus dem Menü **Laufwerksverwaltung** der Konsole
- aus dem Bereich **Aktionen** auf der Seitenleiste **Aktionen und Werkzeuge**

*Beachten Sie, dass die Liste verfügbarer Aktionen im Kontextmenü, im Menü **Auswahl** und im Seitenleistenbereich **Aktionen** vom ausgewählten Volume- oder Laufwerkstyp abhängt. Dasselbe trifft auch für nicht zugeordneten Speicher zu.*

Ergebnisanzeige von Aktionen

Die Ergebnisse aller geplanten Festplatten- oder Laufwerksaktionen werden sofort in der Ansicht **Laufwerksverwaltung** der Konsole angezeigt. Wenn Sie z.B. ein Laufwerk erstellen, wird dies sofort angezeigt – und zwar sowohl in der Tabelle als auch in der unteren, grafischen Ansicht. Auch alle anderen Laufwerksänderungen, inklusive geänderter Laufwerksbuchstaben oder -bezeichnungen, werden sofort in der Ansicht dargestellt.

10.6 Festplattenaktionen

Acronis Disk Director Lite ermöglicht folgende auf Festplatten anwendbare Aktionen:

- Disk Initialisierung (S. 207) – richtet neue, dem System hinzuzufügende Hardware ein
- Einfaches Festplatten-Klonen (S. 208) – überträgt die kompletten Daten einer Quell- auf eine Zielplatte (Basisdatenträger vom MBR-Typ)

- Festplatten konvertieren: MBR zu GPT (S. 210) – konvertiert eine MBR-Partitionstabelle zu GPT
- Festplatten konvertieren: GPT zu MBR (S. 211) – konvertiert eine GPT-Partitionstabelle zu MBR
- Festplatten konvertieren: Basis zu Dynamisch (S. 211) – konvertiert einen Basis- zu einem dynamischen Datenträger
- Festplatten konvertieren: Dynamisch zu Basis (S. 212) – konvertiert einen dynamischen zu einem Basisdatenträger

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Festplatten.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf das Ziellaufwerk. Das bedeutet, dass dann auch kein anderes Disk ManagementLaufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass das Laufwerk nicht blockiert werden kann, so schließen Sie das die Platte gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung das Laufwerk gerade blockiert.

10.6.1 Festplatten-Initialisierung

Wenn Sie dem System eine neue Festplatte hinzufügen, so erkennt Acronis Disk Director Lite die veränderte Konfiguration und integriert die neue Platte in die Liste aktueller Laufwerke und Volumes. Sollte die Festplatte noch nicht initialisiert sein oder ein unbekanntes Dateisystem verwenden, so können Sie noch keine Programme auf ihr installieren und keine Daten auf ihr speichern.

In diesem Fall wird Acronis Disk Director Lite erkennen, dass die Festplatte verwendet werden kann, und die Notwendigkeit, diese zu initialisieren. Das Fenster **Laufwerksverwaltung** stellt die neu erkannte Hardware als grauen Balken mit grauem Symbol dar, um so die Nichtverwendbarkeit zu visualisieren.

So initialisieren Sie ein Laufwerk:

1. Wählen das zu initialisierende Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das gewählte Volume und wählen Sie im Kontextmenü **Initialisieren**. Das nachfolgende Fenster **Disk-Initialisierung** versorgt Sie mit grundlegenden Hardware-Details wie Laufwerksnummer oder Kapazität und bietet an, Sie bei der Wahl Ihrer nun möglichen Aktionen zu unterstützen.
3. Sie können in diesem Fenster das Partitionsschema der Disk (MBR oder GPT) und den Disk-Typ (Basis oder Dynamisch) einstellen. Die neue Laufwerksstatus wird sofort grafisch in der **Laufwerksverwaltung**-Ansicht der Konsole angezeigt.
4. Indem Sie auf **OK** klicken, fügen Sie die Disk-Initialisierung der Liste ausstehender Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Nach der Initialisierung bleibt der ganze Festplattenplatz unzugeorndet und kann daher für die Programminstallation oder zur Dateiaufbewahrung nicht benutzt zu werden. Um den Speicherplatz verfügbar zu machen, fahren Sie nun normalerweise mit der Aktion **Volume erstellen** fort.

Wenn Sie weitere Einstellungen des Laufwerks ändern wollen, so können Sie dafür auch später noch die Werkzeuge von Acronis Disk Director Lite verwenden.

10.6.2 Einfaches Festplatten-Klonen

Manchmal ist es notwendig, alle Daten einer Festplatte auf eine andere zu übertragen. Typische Gründe sind eine Vergrößerung des Systemlaufwerks, die Einrichtung eines neuen Systems oder die Räumung des Laufwerks aufgrund eines Hardware-Fehlers. Wie auch immer: die Gründe für die Aktion **Basisdatenträger klonen** können als Notwendigkeit zum exakten Transfer aller Daten einer Quell- auf eine Zielplatte zusammengefasst werden.

Acronis Disk Director Lite ermöglicht Ihnen die Durchführung der Aktion nur mit Basisdatenträgern mit MBR-Partitionsschema.

So planen Sie die Aktion **Basisdatenträger klonen**:

1. Wählen Sie die zu klonende Festplatte.
2. Bestimmen Sie die Zielfestplatte für die Klonaktion.
3. Wählen Sie die Methoden zum Klonen und spezifizieren Sie zusätzliche Optionen.

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

*Es wird empfohlen, einen aktivierten Acronis Startup Recovery Manager (S. 293) (ASRM) zu deaktivieren, bevor Sie ein Systemlaufwerk klonen. Andernfalls könnte das geklonte Betriebssystem möglicherweise nicht starten. Nach dem Klonen können Sie den ASRM aktivieren. Wenn die Deaktivierung nicht möglich ist, dann wählen Sie die Methode **Wie vorliegend**, um die Festplatte zu klonen.*

10.6.2.1 Quell- und Zielfestplatten bestimmen

Das Programm zeigt eine Liste aller partitionierten Laufwerke und fordert den Anwender dann auf, die Quelle zu wählen, von der die Daten zu einer anderen Platte übertragen werden.

Als Nächstes folgt die Wahl der Zielfestplatte für die Klonaktion. Das Programm ermöglicht die Wahl nur solcher Laufwerke, deren Größe ausreichend ist, um alle Daten des Quelllaufwerks verlustfrei aufzunehmen.

Sollten sich auf der gewählten Zielfestplatte Daten befinden, wird eine Warnung angezeigt: "**Das gewählte Ziellaufwerk ist nicht leer. Die Daten auf dem Laufwerk werden überschrieben.**", was bedeutet, dass alle derzeit auf dem gewählten Laufwerk verfügbaren Daten unwiederbringlich verloren gehen.

10.6.2.2 Klon-Methoden und erweiterte Optionen

Die Aktion **Basis-Laufwerk klonen** bedeutet normalerweise, dass alle Informationen des Quelllaufwerks "**Wie vorliegend**" auf das Ziellaufwerk übertragen werden. Sollte also das Zielllaufwerk gleich groß oder größer sein, so können alle Informationen exakt wie auf der Quelle gespeichert übertragen werden.

Durch die große Bandbreite verfügbarer Hardware ist es jedoch durchaus normal, dass das Ziellaufwerk eine andere Größe als die Quelle hat. Sollte das Ziellaufwerk größer sein, so kann es ratsam sein, unter Verwendung der Option **Volumes proportional anpassen** die Quelllaufwerke so anzupassen, dass auf dem Ziel nicht zugeordneter Speicherplatz vermieden wird. Die Option **Basisdatenträger klonen** „wie vorliegend" bleibt bestehen, nur wird die Standardmethode zum Klonen inkl. proportionaler Vergrößerung aller **Quell-**-Laufwerke so durchgeführt, dass auf der **Ziel**-Festplatte kein nicht zugeordneter Speicherplatz verbleibt.

Ist das Ziel kleiner, so steht die Option **Wie vorliegend** nicht mehr zur Verfügung wird die proportionale Größenanpassung **Quell**-Laufwerke zwingend notwendig. Das Programm analysiert das

Ziellaufwerk daraufhin, ob seine Größe ausreicht, alle Daten des **Quelllaufwerks** verlustfrei aufnehmen zu können. Nur wenn ein Transfer mit proportionaler Größenanpassung der **Quell**-Laufwerke ohne Datenverlust möglich ist, kann der Anwender mit der Aktion fortfahren. Sollte wegen einer Größenbeschränkung eine sichere Übertragung der **Quell**-Daten auf das **Ziel**-Laufwerk auch mit proportionaler Größenanpassung nicht möglich sein, dann die Aktion **Basis-Laufwerk klonen** nicht mehr fortgesetzt werden.

Wenn Sie vorhaben, ein Laufwerk zu klonen, das ein **System-Volume** enthält, sollten Sie die **Erweiterten Optionen** beachten.

Indem Sie auf **Abschluss** klicken, fügen Sie das Laufwerk-Klonen der Liste ausstehender Aktionen hinzu.

(Damit die hinzugefügte Aktion durchgeführt werden, müssen Sie diese ausführen (S. 220) lassen. Wenn Sie das Programm ohne Ausführung der offenen Aktionen beenden, werden diese alle verworfen.)

Erweiterte Optionen verwenden

Wenn Sie ein Laufwerk klonen, das ein **System-Volume** enthält, müssen Sie auch die Bootfähigkeit des Betriebssystems für das Ziellaufwerk bewahren. Das bedeutet, dass das Betriebssystem System-Laufwerks-Informationen (z.B. Laufwerksbuchstabe) erhalten muss, die zur NT-Festplatten-Signatur passen (welche im Master Boot Record hinterlegt ist). Zwei Festplatten mit derselben NT-Signatur können jedoch nicht richtig unter einem Betriebssystem arbeiten.

Wenn aber auf einer Maschine zwei Festplatten, die ein System-Laufwerk enthalten, dieselbe NT-Signatur haben, so startet das Betriebssystem von der ersten Festplatte, erkennt dabei die gleiche Signatur auf der zweiten Festplatte, erzeugt automatisch eine neue, eindeutige NT-Signatur und weist diese dann der zweiten Platte zu. Als Konsequenz verlieren darauf dann alle Volumes des zweiten Laufwerks ihre Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf diesem Laufwerk kann daher auch nicht mehr booten.

Ihnen stehen zwei Alternativen zur Verfügung, um die Bootfähigkeit auf dem Ziellaufwerk zu erhalten:

1. Kopieren der NT-Signatur – um die Zielfestplatte mit der NT-Signatur zu versehen, die zu den ebenfalls auf die Platte kopierten Registry-Schlüsseln passt
2. NT-Signatur belassen – um die alte Disk-Signatur des Ziellaufwerks zu bewahren und das Betriebssystem an diese anzupassen

Falls Sie die NT-Signatur kopieren müssen:

1. Aktivieren Sie das Kontrollkästchen **NT-Signatur kopieren**. Sie erhalten eine Warnung: "Wenn sich auf der Festplatte ein Betriebssystem befindet, so entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer, bevor Sie diesen erneut starten. Anderenfalls wird das Betriebssystem von der ersten der beiden Festplatten starten und das Betriebssystem der zweiten Platte seine Bootfähigkeit verlieren." Das Kontrollkästchen **Computer nach dem Klonen ausschalten** hat den Fokus und ist automatisch deaktiviert.
2. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
3. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
4. Warten Sie dann, bis die Aktion beendet ist.
5. Und danach, bis der Computer ausgeschaltet wird.
6. Entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer.
7. Schalten Sie den Computer wieder ein.

Falls Sie die NT-Signatur bewahren müssen:

1. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **NT-Signatur kopieren**.
2. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **Computer nach dem Klonen ausschalten**.
3. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
4. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
5. Warten Sie dann, bis die Aktion beendet ist.

10.6.3 Festplatten konvertieren: MBR zu GPT

In folgenden Fällen kann es angebracht sein, einen MBR- in einen GPT-Basisdatenträger zu konvertieren:

- Wenn Sie mehr als 4 primäre Laufwerke auf einem Laufwerk benötigen.
- Wenn Sie die Zuverlässigkeit der Festplatte gegen möglichen Datenverlust erhöhen müssen.

Wenn Sie einen MBR- in einen GPT-Basisdatenträger konvertieren müssen:

1. Bestimmen Sie den MBR-Basisdatenträger, der zu GPT konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu GPT konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von MBR nach GPT zu konvertieren.
3. Indem Sie auf **OK** klicken, fügen Sie MBR-zu-GPT-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Beachten Sie: Ein GPT-partitioniertes Laufwerk reserviert am Ende des partitionierten Bereiches Speicherplatz für einen benötigten Backupbereich, in dem Kopien des GPT-Headers und der Partitionstabelle gespeichert werden. Sollte die Festplatte so voll sein, dass keine automatische Verringerung der Laufwerksgröße möglich ist, so wird die MBR-zu-GPT-Konvertierung fehlschlagen.

Die Aktion kann außerdem nicht rückgängig gemacht werden. Wenn Sie eine MBR-Festplatte mit einer primären Partition haben, diese erst zu GPT und dann wieder zurück zu MBR konvertieren, so wird die Partition zu einem logischen Laufwerk, welches dann nicht mehr als Systempartition verwendet werden kann.

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Rückkonvertierung der Festplatte zu MBR über dasselbe Menü möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Konvertierung dynamischer Datenträger: MBR zu GPT

Eine direkte MBR-zu-GPT-Konvertierung von dynamischen Datenträgern wird von Acronis Disk Director Lite nicht unterstützt. Sie können jedoch zum selben Ziel kommen, wenn Sie die folgenden Konvertierungen durchführen:

1. MBR Festplatten-Konvertierung: Dynamisch zu Basis (S. 212) unter Verwendung der Aktion **Zu Basis konvertieren**.
2. Konvertierung von Basisdatenträgern: MBR zu GPT durch Verwendung der Aktion **Zu GPT konvertieren**.
3. GPT Festplatten-Konvertierung: Basis zu Dynamisch (S. 211) durch Verwendung der Aktion **Zu Dynamisch konvertieren**.

10.6.4 Festplatten konvertieren: GPT zu MBR

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Konvertierung der GPT-Platte zu MBR möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Wenn Sie eine GPT-Festplatte zu MBR konvertieren müssen:

1. Bestimmen Sie die GPT-Festplatte, die zu MBR konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu MBR konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von GPT nach MBR zu konvertieren.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Lafuwerk von GPT zu MBR konvertiert wird. Z.B., dass die Konvertierung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch das Betriebssystem nicht mehr starten kann – oder dass auf manche Volumes des gewählten GPT-Laufwerks im MBR-Modus nicht mehr zugegriffen werden kann (weil diese jenseits der 2 TByte-Grenze liegen).

   Beachten Sie, dass ein zu einer GPT-Festplatte gehörendes Laufwerk nach der irreversiblen Konvertierung zu einer logischen Partition wird.

3. Indem Sie auf **OK** klicken, fügen Sie die GPT-zu-MBR-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

10.6.5 Festplatten konvertieren: Basis zu Dynamisch

In folgenden Fällen ist eine Konvertierung von Basis- zu dynamischen Datenträgern angebracht:

- Wenn Sie die Festplatte als Teil einer dynamischen Laufwerksgruppe verwenden wollen.
- Wenn Sie eine erhöhte Zuverlässigkeit der Datenspeicherung auf der Festplatte erreichen wollen.

Wenn Sie einen Basis- zu einem dynamischen Datenträger konvertieren müssen:

1. Wählen Sie den zu konvertierenden Basisdatenträger.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu Dynamisch konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Basis zu Dynamisch ansteht.
3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt und falls notwendig der Computer neu gestartet.

   Beachten Sie: Ein dynamischer Datenträger belegt das letzte Megabyte des physikalischen Laufwerks mit einer Datenbank, die eine so genannte Four-Level-Beschreibung (Volume-Component-Partition-Disk) für jedes dynamische Laufwerk enthält. Sollte sich während der Konvertierung zu Dynamisch herausstellen, dass der Basisdatenträger voll ist und daher die Laufwerksgröße nicht automatisch reduziert werden kann, so schlägt die Konvertierungsaktion fehl.

Sollten Sie irgendwann den dynamischen wieder zu einem Basisdatenträger zurückwandeln wollen, etwa um ein Betriebssystem zu verwenden, welches dynamische Datenträger nicht unterstützt, so können Sie dafür dasselbe Menü verwenden (wobei der Aktionsbefehl **Zu Basis konvertieren** lautet).

Konvertierung eines System-Laufwerkes

Acronis Disk Director Lite benötigt nach einer Basis-zu-Dynamisch-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf der Festplatte nur ein Betriebssystem vom Typ Windows Server 2008/Vista vorhanden ist.
2. Auf dem Computer dieses Betriebssystem läuft.

Die Konvertierung von 'Basis' zu 'Dynamisch' eines Laufwerks, das eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager bewahrt das Programm die Bootfähigkeit eines **Offline-Betriebssystems** nach der Aktion.

10.6.6 Laufwerk konvertieren: Dynamisch zu Basis

Eine Rückkonvertierung von dynamischen zu Basis-Laufwerken ist z.B. dann angebracht, wenn Sie ein Betriebssystem verwenden wollen, dass dynamische Laufwerke nicht unterstützt.

Wenn Sie ein Laufwerk von 'Dynamisch' zu 'Basis' konvertieren müssen:

1. Wählen Sie das zu konvertierende dynamische Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu 'Basis' konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Dynamisch zu Basis ansteht.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Laufwerk vom Typ 'Dynamisch' zu 'Basis' konvertiert wird. Z. B. dass die Umwandlung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch ein Betriebssystem nicht mehr starten kann – oder dass Sie für den Fall, dass das zu konvertierende Laufwerke Volumes von einem Typ enthält, die nur von dynamischen Laufwerken unterstützt werden (alle Laufwerkstypen außer Volumes vom Typ 'Einfach') über den möglichen Verlust von Daten infolge der Konvertierung gewarnt werden.

   Beachten Sie, dass die Aktion nicht auf dynamische Laufwerke angewendet werden kann, die übergreifende, Stripeset- oder RAID-5-Volumes enthalten.

3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt.

Nach der Umwandlung werden 8 MB des Laufwerksspeichers für zukünftige Konvertierungen von Basis zu Dynamisch reserviert.

Der resultierende nicht zugeordnete Speicherplatz und die anvisierte maximale Volume-Größe können von Fall zu Fall variieren (z.B. weil die Größe einer Spiegelung die Größe einer anderen Spiegelung bedingt oder weil die letzten 8 MB Speicherplatz für zukünftige Konvertierungen von 'Basis' zu 'Dynamisch' reserviert werden).

Systemlaufwerk konvertieren

Acronis Disk Director Lite benötigt nach einer Dynamisch-zu-Basis-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf dem Laufwerk ist nur ein Betriebssystem vom Typ Windows Server 2008/Vista installiert.
2. Die Maschine dieses Betriebssystem ausführt.

Die Dynamisch-zu-Basis-Konvertierung Festplatte, die eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager gewährleistet das Programm:

- sichere Konvertierung eines dynamischen zu einem Basis-Laufwerk, sofern dieses Laufwerk Volumes **mit Daten** für einfache und gespiegelte Volumes enthält.

- in Multiboot-Systemen die Bootfähigkeit eines Systems, das während der Aktion **offline** war.

10.6.7 Laufwerkstatus ändern

Die Funktion 'Laufwerkstatus ändern' gilt für die Betriebssysteme Windows Vista SP1+, Windows Server 2008 und Windows 7 und bezieht sich auf die aktuelle Laufwerksstruktur (S. 205).

Der Laufwerksstatus erscheint immer in der grafischen Anzeige des Laufwerks neben dem Laufwerksnamen; es gibt folgende Möglichkeiten:

- **Online**
  Der Status 'online' bedeutet, dass auf das Laufwerk im Modus Lesen-Schreiben zugegriffen werden kann. Dies ist der normale Laufwerkstatus. Wenn das Laufwerk nur im Lesemodus verfügbar sein soll, wählen Sie das Laufwerk aus und ändern Sie den Status zu 'offline'; wählen Sie dazu **Disk-Status zu offline ändern** im Menü **Aktionen**.
- **Offline**
  Der Status 'offline' bedeutet, dass auf das Laufwerk nur im Lesemodus zugegriffen werden kann. Um den Modus des gewählten Laufwerks von offline zurück zu online zu ändern, wählen Sie **Disk-Status auf online ändern** im Menü **Aktionen**.
  Wenn ein Laufwerk den Status offline hat und der Laufwerkname als **Fehlend** angegeben ist, kann das Betriebssystem dieses Laufwerk nicht finden bzw. nicht identifizieren. Es ist möglicherweise defekt, getrennt oder abgeschaltet. Informationen darüber, wie Sie ein als fehlend und offline gekennzeichnetes Laufwerk wieder in den Status online bringen, finden Sie in diesem Artikel in der Microsoft Knowledge Base:
  http://technet.microsoft.com/de-de/library/cc732026%28WS.10%29.aspx .

10.7 Aktionen für Volumes

Acronis Disk Director Lite ermöglicht folgende auf Partitionen anwendbare Aktionen:

- Partition erstellen (S. 213) – erstellt neue Partitionen mit Hilfe des Assistenten zur Partitionserstellung
- Partition löschen (S. 218) – löscht eine gewählte Partition
- Aktiv setzen (S. 218) – kennzeichnet eine gewählte Partition als „Aktiv“, so dass ein hier installiertes Betriebssystem gebootet werden kann.
- Laufwerksbuchstaben ändern (S. 219) – wechselt den Laufwerksbuchstaben der gewählten Partition
- Bezeichnung ändern (S. 219) – ändert die Datenträgerbezeichnung der gewählten Partition
- Volume formatieren (S. 220) – formatiert ein Volume mit einem benötigten Dateisystem

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Partitionen.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf die Zielpartition. Das bedeutet, dass dann auch kein anderes Laufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass die Partition nicht blockiert werden kann, so schließen Sie das die Partition gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung die Partition gerade blockiert.

10.7.1 Eine Partition erstellen

Beispiele, wann eine neue Partition benötigt wird:

- Wiederherstellung eines früher gesicherten Backups mit exakt derselben Konfiguration;
- separate Speicherung von Sammlungen ähnlicher Dateien – z.B. Sammlungen von MP3- oder Videodateien auf einer separaten Partition;
- Sicherung der Backups (Images) anderer Partitionen/Festplatten auf einem besonderen Laufwerk;
- Installation eines neuen Betriebssystems (oder einer Auslagerungsdatei) auf einer neuen Partition;
- Hinzufügen neuer Hardware zu einem Computer.

Das Werkzeug zum Erstellen neuer Partitionen in Acronis Disk Director Lite ist der **Assistent zur Partitionserstellung**.

10.7.1.1 Verschiedene Arten dynamischer Volumes

Einfaches Volume (Simple)

Ein Laufwerk, das vom freien Speicherplatz eines einzelnen physikalischen Laufwerks erstellt wurde. Es kann aus einer oder auch mehreren Regionen auf der Festplatte bestehen, die durch den „Logical Disk Manager“ (LDM) von Windows virtuell vereint werden. Es stellt keine zusätzlichen Vorteile bereit, weder bei der Geschwindigkeit noch bei der Größe.

Übergreifendes Volume (Spanned)

Ein Laufwerk, basierend auf dem freien Speicher mehrerer physikalischer Festplatten, die durch den LDM miteinander verbunden sind. Bis zu 32 Laufwerke können zu einen Volume integriert werden, was zwar einerseits Hardware-Größenbeschränkungen sprengt, aber andererseits auch bedingt, dass bei Ausfall nur eines Laufwerks die Gesamtheit aller Daten verloren geht und kein Teil dieses übergreifenden Laufwerkes entfernt werden kann, ohne dass das ganze Laufwerk zerstört wird. Daher bringt ein übergreifendes Volume weder eine bessere Zuverlässigkeit, noch eine bessere E/A-Rate.

Stripeset-Volume

Ein manchmal auch RAID-0 genanntes Laufwerk, das aus gleich großen „Daten-Stripesets“ besteht, die quer über alle verwendeten Laufwerke geschrieben werden; was bedeutet, dass Sie zur Erstellung eines Stripeset-Volumes zwei oder mehr dynamische Laufwerke benötigen. Die Laufwerke in einem Volume vom Typ 'Stripeset' müssen nicht identisch sein, aber auf jeder Laufwerk, das Sie in das Volume aufnehmen wollen, muss ungenutzter Speicher vorhanden sein und die Größe des Volumes wird bestimmt durch die Größe des kleinsten Speicherplatzes. Der Datenzugriff bei einem Volume vom Typ 'Stripeset' ist üblicherweise schneller als der vergleichbare Zugriff auf ein einziges physikalisches Laufwerk, weil die Eingabe/Ausgabe-Operationen über mehr als ein Laufwerk verteilt werden.

Laufwerke vom Typ 'Stripeset' werden zur Performance-Steigerung und nicht wegen besserer Zuverlässigkeit erstellt, da sie keine redundanten Informationen enthalten.

Gespiegeltes Volume (Mirrored)

Ein manchmal auch RAID-1 genannter, fehlertoleranter Laufwerkstyp, dessen Daten auf zwei identischen physikalischen Festplatten dupliziert werden. Alle Daten des einen Laufwerks werden zur Schaffung der Datenredundanz auf das andere Laufwerk kopiert. Nahezu jedes Laufwerk kann gespiegelt werden, einschließlich System- und Boot-Laufwerke – falls der Laufwerke ausfällt, kann immer noch auf die Daten des verbliebenen Laufwerks zugegriffen werden. Leider gibt es starke Hardware-Begrenzungen bezüglich Größe und Geschwindigkeit bei der Verwendung von gespiegelten Volumes.

Gespiegeltes Stripeset-Volume

Ein auch RAID-1+0 genanntes, fehlertolerantes Volume, welches die Vorteile erhöhter E/A-Geschwindigkeit des Typs 'Stripeset' mit der Redundanz beim Typ 'Gespiegelt' kombiniert. Was jedoch bleibt, ist ein offensichtlicher, von der 'Spiegelung'-Architektur stammender Nachteil: ein schlechtes Laufwerk-zu-Volume-Größenverhältnis.

RAID-5

Ein fehlertolerantes Stripeset-Volume, dessen Daten über eine Zusammenstellung (Array) von drei oder noch mehr Laufwerken quer verteilt sind. Die Festplatten müssen nicht identisch sein, aber jede Festplatte des „Volumes" muss über gleich große Blöcke an nicht zugeordnetem Speicherplatz verfügen. Außerdem werden über das Laufwerk-Array auch Paritätsdaten (speziell berechnete Werte, die im Fehlerfall zur Datenrekonstruktion verwendet werden können) verteilt gespeichert. Und diese Paritätsdaten werden immer auf einem anderen Laufwerk als die eigentlichen Daten gespeichert. Sollte eine physikalische Platte ausfallen, so kann der Anteil des RAID-5-Laufwerks, der auf dieser Festplatte lag, aus den verbliebenen Daten und den Paritätsdaten wiederhergestellt werden. Ein RAID-5-Volume bietet erhöhte Zuverlässigkeit und ermöglicht die Speicherbegrenzungen physikalischer Laufwerke zu überwinden, wobei das Disk-zu-Volume-Größenverhältnis besser ist als bei Laufwerken vom Typ 'Gespiegelt' (Mirrored).

10.7.1.2 Der Assistent zur Partitionserstellung

Der Assistent zur **Partitionserstellung** ermöglicht Ihnen, jeden Partitionstyp (inkl. System und Aktiv) anzulegen, ein Dateisystem zu wählen, einen Laufwerksbuchstaben zuzuweisen und noch weitere Laufwerksverwaltung-Funktionen zu verwenden.

Sie können Schritt für Schritt Aktionsparameter eingeben und jederzeit für Korrekturen auch wieder zu vorherigen Schritten zurückwechseln. Um Sie bei Ihrer Wahl zu unterstützen, ist jeder Parameter mit detaillierten Anweisungen ergänzt.

So erstellen Sie eine neue Partition:

Starten Sie den **Assistenten zur Partitionserstellung** durch Wahl des Befehls **Partition erstellen** im Seitenleistenbereich **Assistenten** – oder rechtsklicken Sie auf einen nicht zugeordneten Speicherplatz und wählen im erscheinenden Kontextmenü **Partition erstellen**.

Bestimmen Sie den zu erstellenden Partitionstyp

In diesem ersten Schritt müssen Sie die Art der Partition spezifizieren, die Sie erstellen wollen. Die folgenden Partitionstypen stehen zur Verfügung:

- Basis
- Einfach/Übergreifend
- Stripset
- Gespiegelt
- RAID-5

Ihnen wird eine kurze Beschreibung für jeden Partitionstyp angezeigt (zum besseren Verständnis der Vorteile und Beschränkungen jeder möglichen Partitionsarchitektur).

*Sollte das aktuelle, auf dem Computer installierte Betriebssystem den gewählten Partitionstyp nicht unterstützen, so erhalten Sie eine entsprechende Warnung. In diesem Fall wird die **Weiter**-Schaltfläche deaktiviert, so dass Sie zum Fortsetzen der Partitionserstellung einen anderen Partitionstyp wählen müssen.*

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Ziellaufwerk wählen (S. 216).

Ziellaufwerk wählen

Der nächste Assistentenschritt fordert Sie auf, die Festplatte zu wählen, deren unzugeordneter Speicher für die Partitionserstellung genutzt wird.

So erstellen Sie ein Basis-Volume:

- Wählen Sie die Zielfestplatte und den nicht zugeordneten Speicherplatz, von dem die Basis-Volume erstellt werden soll.

So erstellen Sie eine einfaches/übergreifendes Volume:

- Wählen Sie eine oder mehrere Zielfestplatten, auf der/denen die Partition erstellt wird.

So erstellen Sie ein gespiegeltes Volume:

- Wählen Sie zwei Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine Stripeset-Volume:

- Wählen Sie zwei oder mehr Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine RAID-5-Partition:

- Wählen Sie drei Ziellaufwerke, auf denen das Volume erstellt wird.

Nach der Wahl der Laufwerke ermittelt der Assistent die maximale Größe des resultierenden Volumes, das sich aus der Menge des auf dem Laufwerk verfügbaren, nicht zugeordneten Speicherplatzes sowie gegebenen Anforderungen des zuvor bestimmten Volume-Typs ableitet.

Wenn Sie versuchen, ein **dynamisches** Laufwerk auf einem oder mehreren **Basisdatenträgern** anzulegen, so erhalten Sie eine Warnmeldung, dass die gewählten Festplatten automatisch zu dynamischen Datenträgern konvertiert werden.

Sofern erforderlich (abhängig vom gewählten Partitionstyp), werden Sie aufgefordert, Ihrer Auswahl eine notwendige Anzahl von Laufwerken hinzuzufügen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Partitionstyp festlegen (S. 215).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Partitionsgröße festlegen (S. 216).

Partitionsgröße festlegen

Auf der dritten Assistentenseite können Sie die Größe der zukünftigen Partition definieren, abhängig von den zuvor gemachten Einstellungen. Um die benötigte Größe innerhalb der minimalen und maximalen Grenzen einzustellen, können Sie den Schieberegler verwenden oder die gewünschten Werte im Eingabefenster eintippen oder die Begrenzungslinien der grafischen Laufwerksdarstellung mit der Maus verschieben.

Bei Verwendung des maximalen Wertes wird normalerweise der gesamte nicht zugeordnete Speicherplatz in die Laufwerkserstellung eingeschlossen. Der resultierende nicht zugeordnete Speicher und die anvisierte maximale Laufwerksgröße können von Fall zu Fall variieren (z.B. weil die Größe einer Mirror-Platte die Größe einer anderen Mirror-Platte bedingt oder weil auf der Festplatte die letzten 8 MB für zukünftige Konvertierungen von Basis zu Dynamisch reserviert werden).

Wenn bei Basis-Partitionen einiger nicht zugeordneter Speicherplatz auf der Festplatte verbleibt, so können Sie außerdem die Position der neuen Partition wählen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Ziellaufwerk wählen (S. 216).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Volume-Optionen einstellen (S. 217).

Volume-Optionen einstellen

Im nächsten Assistentenschritt können Sie einen **Laufwerksbuchstaben** zuweisen (Standard ist der erste freie Buchstabe im Alphabet) und optional die **Datenträgerbezeichnung** (Standard ist keine Bezeichnung). Hier spezifizieren Sie außerdem das **Dateisystem** und die **Clustergröße**.

Der Assistent fordert Sie auf, eines der Windows-Dateisysteme zu wählen: FAT16 (bei Partitionsgrößen über 2 GB deaktiviert), FAT32 (bei Partitionsgrößen über 2 TB deaktiviert), NTFS oder Sie lassen die Partition **Unformatiert**.

Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.

Beim Erstellen einer Basis-Volume, die auch als System-Volume verwendet werden kann, offeriert der Assistent eine geänderte Anzeige mit der Möglichkeit, den **Partitionstyp** auf **Primär**, **Aktiv** oder **Logisch** einzustellen.

Primär ist die gängige Wahl, wenn ein Betriebssystem auf dem Volume installiert werden soll. Wählen Sie **Aktiv**, wenn Sie auf dem Volume ein Betriebssystem installieren wollen, von dem der Computer beim Start direkt bootet. Wenn die Einstellung **Primär** nicht ausgewählt ist, so ist auch die Option **Aktiv** ausgeschaltet. Soll das Volume nur zum Speichern von Daten verwendet werden, so wählen Sie **Logisch**.

*Ein Basisdatenträger kann bis zu vier primäre Volumes enthalten. Sollten diese schon existieren, so muss das Laufwerk zur Erstellung weiterer primärer Volumes in ein dynamisches Volume konvertiert werden – anderenfalls sind die Einstellungen **Aktiv** und **Primär** deaktiviert und Sie können nur den Volume-Typ **Logisch** wählen. Durch eine Warnmeldung werden Sie gegebenenfalls darauf hingewiesen, dass von diesem Volume nicht gebootet werden kann.*

*Wenn Sie für eine neue Datenträgerbezeichnung Ziffern verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie auch eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Sie müssen die Bezeichnung ändern, um mit der Erstellung des neuen Volumes fortzufahren.*

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Partitionsgröße festlegen (S. 216).

Durch Klicken auf **Abschluss** wird die geplante Aktion abgeschlossen.

Zur Abarbeitung der geplanten Aktion klicken Sie zuerst auf **Ausführen** in der Symbolleiste und dann auf **Fertig stellen** im erscheinenden Fenster **Ausstehende Aktionen.**

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

10.7.2 Volume löschen

Diese Version von Acronis Disk Director Lite hat eine reduzierte Funktionalität, weil sie hauptsächlich zur Vorbereitung fabrikneuer Systeme für die Wiederherstellung zuvor gesicherter Partitionsabbilder gedacht ist. Funktionen zur Größenänderung bestehender Partitionen und zur Erstellung neuer Partitionen unter Verwendung des Speicherplatzes bereits vorhandener Partitionen finden sich nur in der Vollversion, so dass mit der vorliegenden Lite-Version das Löschen von Partitionen manchmal der einzige Weg sein kann, um benötigten Festplattenplatz ohne Veränderung der Festplattenkonfiguration freizugeben.

Nachdem eine Partition gelöscht wurde, wird sie dem nicht zugeordneten Speicherplatz der Platte hinzugefügt. Das lässt sich nutzen, um eine neue Partition zu erstellen oder den Partitionstyp einer anderen zu verändern.

So löschen Sie eine Partition:

1. Wählen Sie eine Festplatte und auf dieser die zu löschende Partition.
2. Wählen Sie den Befehl **Partition löschen** oder einen entsprechenden Eintrag in der **Aktionen**-Liste der Seitenleiste – oder klicken Sie auf das Symbol **Partition löschen** in der Symbolleiste.

   Sollten sich auf der Partition Daten befinden, so werden Sie mit einer Meldung gewarnt, dass alle Informationen unwiederbringlich verloren gehen.

3. Indem Sie im Fenster **Partition löschen** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

10.7.3 Die aktive Partition setzen

Wenn Sie über mehrere primäre Partitionen verfügen, so müssen Sie eine davon als Boot-Partition spezifizieren. Dafür können Sie die Partition so einstellen, dass sie „aktiv" wird. Auf einer Festplatte kann jedoch nur ein Laufwerk aktiv sein: wird eine Partition neu als aktiv gesetzt, dann wird bei einer zuvor aktiven Partition die entsprechende Einstellung aufgehoben.

So setzen Sie eine Partition aktiv:

1. Bestimmen Sie eine primäre Partition auf einem MBR-Basisdatenträger, die aktiv gesetzt werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Aktiv setzen**.

   Sofern keine andere aktive Partition im System vorliegt, wird die Operation zur Liste der ausstehenden Aktionen hinzugefügt.

   Beachten Sie, dass sich durch das Aktivsetzen der neuen Partition wiederum der Laufwerksbuchstabe einer zuvor aktiven Partition ändern kann und daher installierte Anwendungsprogramme evtl. nicht mehr lauffähig sein können.

3. Sollte im System eine andere Partition aktiv sein, so erhalten Sie eine Warnmeldung, dass diese bisherige aktive Partition zuerst auf passiv gesetzt werden muss. Indem Sie im **Warndialog** auf **OK** klicken, wird das Setzen der aktiven Partition zur Liste ausstehender Aktionen hinzugefügt.

   Beachten Sie: Selbst wenn ein Betriebssystem auf der neuen aktiven Partition liegt, kann es unter Umständen sein, dass der Computer dennoch nicht von ihr booten kann. Sie müssen Ihre Entscheidung bestätigen, damit die neue Partition als aktiv gesetzt wird.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.4 Laufwerksbuchstaben ändern

Das Windows-Betriebssystem weist Festplatten-Laufwerken ihre Laufwerksbuchstaben während des Startvorgangs zu. Diese Laufwerksbuchstaben werden vom Betriebssystem und Anwendungsprogrammen verwendet, um Dateien und Ordner auf den Partitionen zu finden.

Das Hinzufügen neuer Festplatten sowie das Erstellen oder Löschen von Partitionen auf existierenden Platten kann Ihre Systemkonfiguration ändern. Das kann zur Folge haben, dass manche Anwendungsprogramme nicht mehr normal funktionieren oder Benutzerdateien nicht mehr automatisch gefunden bzw. geöffnet werden können. Um dem entgegenzuwirken, können Sie vom Betriebssystem auf die Partitionen zugewiesene Laufwerksbuchstaben manuell ändern.

So ändern Sie den Laufwerksbuchstaben einer Partition, der vom Betriebssystem zugewiesen wurde:

1. Wählen Sie die Partition, deren Laufwerksbuchstabe geändert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Laufwerksbuchstabe ändern**.
3. Wählen Sie im Dialog **Laufwerksbuchstabe ändern** den neuen Laufwerksbuchstaben.
4. Indem Sie im Fenster **Laufwerksbuchstabe ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.5 Volume-Bezeichnung ändern

Die Bezeichnung eines Volumes ist ein optionales Attribut. Es handelt sich um einen Namen, der dem Volume zur leichteren Erkennung zugeordnet wird. So kann z.B. ein Volume SYSTEM genannt werden (Volume für das Betriebssystem) oder PROGRAMME (Volume für Anwendungen) oder DATEN (Volume für Dokumente), was jedoch nicht bedeutet, dass auf diesem Volume nur noch Daten gespeichert werden können, die dieser Bezeichnung entsprechen.

Unter Windows werden die Volume-Bezeichnungen im Verzeichnisbaum des Explorers angezeigt: Laufwerk1(C:), Laufwerk2(D:), Laufwerk3(E:), etc. Laufwerk1, Laufwerk2 und Laufwerk3 sind Volume-Bezeichnungen. Eine Volume-Bezeichnung ist außerdem auch in den Öffnen-/Speichern-Dialogen aller Anwendungsprogramme sichtbar.

So ändern Sie die Bezeichnung eines Volumes:

1. Rechtsklicken Sie auf das gewünschte Volume und wählen Sie **Bezeichnung ändern**.
2. Geben Sie in das Textfeld des Dialoges **Bezeichnung ändern den neuen Laufwerksnamen ein.**
3. Indem Sie im Fenster **Bezeichnung ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   *Wenn Sie für die neue Bezeichnung des Volumes Zeichen verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Um mit der Änderung der Volume-Bezeichnung fortfahren zu können, dürfen Sie für die Aktion nur noch unterstützte Zeichen verwenden.*

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Bezeichnung wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.6 Volume formatieren

Fälle, in denen es angebracht sein kann, ein Volume mit einem neuen Dateisystem zu formatieren:

- Um zusätzlichen Speicherplatz zu gewinnen, der zuvor durch eine ungünstige Clustergröße auf FAT16- oder FAT32-Dateisystemen verloren ging.
- Um auf dem Volume befindliche Daten auf schnelle und relativ verlässliche Art zu zerstören

So formatieren Sie ein Volume:

1. Wählen Sie das zu formatierende Volume.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Volume und wählen Sie im Kontextmenü **Formatieren**.

   Darauf erscheint das Fenster **Volume formatieren**, in dem Sie die Einstellungen für das neue Dateisystem vornehmen können. Sie können eines der Windows-Dateisysteme wählen: FAT16 (bei Volume-Größen über 2 GB deaktiviert), FAT32 (bei Volume-Größen über 2 TB deaktiviert) oder NTFS.

   Falls notwendig, können Sie im Textfeld für das Volume eine Bezeichnung eingeben: standardmäßig ist dieses Fenster leer.

   Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.
3. Wenn Sie auf **OK** klicken, um mit dem Befehl **Volume formatieren** fortzufahren, wird dieser der Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 220). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Volume-Struktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

10.8 Ausstehende Aktionen

Alle vom Anwender manuell oder mit Hilfe eines Assistenten zusammengestellten Aktionen werden solange als ausstehend angesehen, bis der Anwender durch Anstoß eines entsprechenden Befehls bewirkt, dass alle Änderungen dauerhaft gemacht werden. Bis dahin visualisiert Acronis Disk Director Lite lediglich die neue Laufwerksstruktur so, wie es sich aus den geplanten, auf Laufwerken und Volumes anzuwendenden Aktionen ergibt. Dieser Ansatz ermöglicht geplante Aktionen zu kontrollieren, beabsichtigte Änderungen doppelt überprüfen zu können und sofern nötig Aktionen vor der Ausführung jederzeit abbrechen zu können.

Das Programm zeigt Ihnen also zuerst eine Liste aller ausstehenden Aktionen an, um Sie vor unbeabsichtigten Änderungen Ihrer Laufwerke zu bewahren.

Sie finden in der Anzeige **Laufwerksverwaltung** eine Symbolleiste, die Icons zum Starten der Befehle **Rückgängig**, **Wiederherstellen** und **Ausführen** enthält, welche speziell für die ausstehenden Aktionen

gedacht sind. Sie können diese Befehle außerdem über das Menü **Disk ManagementLaufwerksverwaltung** der Konsole starten.

Alle geplanten Operationen werden zur Liste der ausstehenden Aktionen hinzugefügt.

Über den Befehl **Rückgängig** können Sie je den letzten Befehl in dieser Liste zurücksetzen. Solange die Liste nicht leer ist, steht dieser Befehl zur Verfügung.

Über den Befehl **Wiederherstellen** können Sie die letzte ausstehende und zuvor rückgängig gemachte Aktion wieder zurückholen.

Der Befehl **Ausführen** bringt Sie zum Fenster **Ausstehende Aktionen**, in dem Sie die Liste dieser ausstehenden Aktionen noch einmal einsehen können. Durch Klick auf **Fertig stellen** wird dann die Ausführung gestartet. Sobald Sie den Befehl **Fertig stellen** gewählt haben, sind Sie jedoch nicht mehr in der Lage, irgendeinen Befehl oder eine Aktion rückgängig zu machen. Sie können die Umsetzung aber vorher durch Klicken auf **Abbrechen** aufheben. In dem Fall werden an der Liste der ausstehenden Aktionen keine Veränderungen durchgeführt.

Da Acronis Disk Director Lite, wenn Sie das Programm ohne die ausstehenden Aktionen auszuführen beenden, alle Aktionen verwirft, erhalten Sie eine entsprechende Warnmeldung, wenn Sie das **Laufwerksverwaltung** einfach verlassen.

11 Anwendungen mit Laufwerk-Backups schützen

Dieser Abschnitt beschreibt, wie Sie ein Laufwerk-Backup verwenden, um auf Windows-Servern laufende Anwendungen zu schützen.

Diese Information gilt für physikalische und virtuelle Maschinen; und auch unabhängig davon, ob die virtuellen Maschinen auf Hypervisor-Ebene oder innerhalb eines Gast-Betriebssystems gesichert werden.

Laufwerk-Backups können eine VSS-kompatible Anwendung potenziell schützen, Acronis hat den Schutz jedoch für folgenden Anwendungen getestet:

- Microsoft Exchange Server
- Microsoft SQL Server
- Active Directory (Active Directory-Domänendienste)
- Microsoft SharePoint

Verwendung eines Laufwerk-Backups auf einem Anwendungsserver

Ein Laufwerk- bzw. Volume-Backup speichert das Dateisystem eines Laufwerks oder Volumes 'als Ganzes'. Daher speichert es alle zum Booten des Betriebssystems erforderlichen Informationen. Es speichert außerdem alle Anwendungsdateien, Datenbankdateien eingeschlossen. Sie können dieses Backup auf verschiedene Arten verwenden, abhängig von der Situation.

- Im Fall eines Desasters können Sie das komplette Laufwerk wiederherstellen, um sicherzustellen, dass das Betriebssytem und alle Anwendungen funktionieren und laufen.
- Sollte das Betriebssystem intakt sein, dann müssen Sie vielleicht eine Anwendungsdatenbank auf ein früheres Stadium zurücksetzen. Stellen Sie dafür die Datenbankdateien wieder her und verwenden Sie die systemeigenen Tools der Anwendung, damit die Datenbank von der Anwendung erkannt und verwendet wird.
- Sie müssen vielleicht nur ein bestimmtes Datenelement extrahieren, beispielsweise ein PDF-Dokument von einem Microsoft SharePoint Server-Backup. Sie können in diesem Fall ein Volume aus einem Backup an das Dateisystem des Anwendungsservers mounten und die systemeigenen Tools der Anwendung verwenden, um das Element zu extrahieren.

11.1 Backup eines Anwendungsservers

Um einen Anwendungsserver schützen zu können, erstellen Sie einen Backup-Plan oder verwenden Sie die Funktion **Backup jetzt** (wie im Abschnitt 'Backup (S. 38)' beschrieben).

Anwendungen, die Datenbanken verwenden, erfordern einige einfache Maßnahmen, um die Konsistenz der Anwendungsdaten innerhalb eines Laufwerk-Backups sicherzustellen.

Backup kompletter Maschinen

Datenbanken können auf mehr als einem Laufwerk oder Volume gespeichert sein. Um sicherzustellen, dass alle benötigten Dateien in einem Backup enthalten sind, sollten Sie die komplette Maschine sichern. Das gewährleistet außerdem, dass die Anwendung weiterhin geschützt bleibt, wenn Sie noch mehr Datenbanken hinzufügen oder zukünftig die Protokolldateien verlagern.

Sollten Sie sicher sein, dass die Datenbanken und damit assoziierte Dateien immer auf denselben Volumes vorliegen, dann möchten Sie möglicherweise nur Backups dieser Volumes erstellen. Oder Sie möchten separate Backup-Pläne für das System-Volume und diejenigen Volumes erstellen,

welche die Daten speichern. Stellen Sie in beiden Fällen sicher, dass alle Volumes, die notwendige Dateien enthalten, in das Backup aufgenommen werden. Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'Datenbankdateien suchen (S. 224)'.

Sollten die Anwendungsdatenbanken sich auf mehreren Maschinen befinden, dann sichern Sie im Backup alle Maschinen mit derselben Planung. Schließen Sie beispielsweise alle SQL Server, die zu einer SharePoint-Farm gehören, in einen zentralen Backup-Plan ein, der nach einer festen Planung läuft.

Volume Shadow Copy (VSS) verwenden

Microsoft Volume Shadow Copy Service (VSS) sollte verwendet werden, um die Konsistenz der Datenbankdateien in einem Backup zu gewährleisten. Ohne VSS würden die Dateien in einem 'crash-konsistenten' Zustand sein; was bedeutet, dass das System nach der Wiederherstellung im gleichen Zustand wäre, als wäre beim Beginn des Backups die Stromversorgung getrennt worden. Während solche Backups für die meisten Anwendungen ausreichend sind, können Anwendungen, die Datenbanken verwenden, von einem 'crash-konsistenten' Zustand aus möglicherweise nicht starten.

Ein VSS Provider benachrichtigt alle VSS-kompatiblen Anwendungen, dass das Backup dabei ist zu starten. Das gewährleistet, dass alle Datenbanktransaktionen dann abgeschlossen sind, wenn Acronis Backup den Daten-Snapshot erfasst. Was wiederum den konsistenten Zustand der Datenbanken im resultierenden Backup sicherstellt.

Acronis Backup kann verschiedene VSS Provider verwenden. Bei Microsoft-Produkten ist der Microsoft Software Shadow Copy Provider (Microsoft-Softwareschattenkopie-Anbieter) die beste Wahl.

VSS auf einer physikalischen Maschine verwenden

Auf einer physikalischen Maschine ist die Verwendung von VSS konfigurierbar. Das gilt außerdem auch für eine virtuelle Maschine, deren Backup innerhalb des Gastbetriebssystems erfolgt. Sie müssen die Verwendung von VSS möglicherweise manuell aktivieren, falls die Werksvoreinstellung vom Standardwert geändert wurde.

Sie müssen außerdem sicherstellen, dass die VSS Writer für die entsprechende Anwendung angeschaltet wurden. Beim Windows Small Business Server 2003 ist der Exchange-Schreiber standardmäßig ausgeschaltet. Informationen zum Anschalten des Schreibers finden Sie im Microsoft Knowledge Base-Artikel http://support.microsoft.com/kb/838183/ .

So aktivieren Sie die standardmäßige Verwendung von VSS für jeden auf einer Maschine erstellten Backup-Plan:

1. Verbinden Sie die Konsole mit der Maschine.
2. Wählen Sie im oberen Menü **Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup** –> **Volume Shadow Copy Service**.
3. Klicken Sie auf **Volume Shadow Copy Service verwenden**.
4. Klicken Sie in der Liste der **Snapshot-Provider** auf **Software – System-Provider**.

Wenn die Konsole mit dem Management Server verbunden ist, können Sie für alle registrierten Maschinen dieselben Standardeinstellungen festlegen.

VSS auf einer virtuellen Maschine verwenden

Beim Backup einer virtuellen Maschine auf Hypervisor-Ebene ist die Verwendung von VSS nicht konfigurierbar. VSS wird immer verwendet, falls die VMware Tools oder die Hyper-V-Integrationsdienste in einem entsprechenden Gast-System installiert sind.

Die Installation dieser Tools/Dienste ist eine allgemeine Voraussetzung für Backups auf Hypervisor-Ebene. Wenn Fehler wie 'stillgelegte Snapshots' (Quiesced Snapshot) beim Backup von virtuellen ESX(i)-Maschinen auftreten, hilft normalerweise ein Neuinstallieren oder ein Update der VMware Tools mit anschließendem Neustart der virtuellen Maschinen. Weitere Informationen finden Sie unter http://kb.acronis.com/content/4559 .

Abschneiden von Transaktionsprotokollen

Active Directory verwendet normalerweise Umlaufprotokollierung. Die Protokolle von anderen VSS-kompatiblen Anwendungen (ausgenommen Microsoft SQL Server) können mithilfe der Option**VSS-Voll-Backup aktivieren** (S. 109) abgeschnitten werden. Diese Option ist nur auf physikalischen und virtuellen Maschinen wirksam, auf denen der Agent für Windows installiert ist.

Andere verfügbare Lösungen beinhalten:

1. Manuelles Abschneiden der Protokolle oder durch Verwendung eines Skripts. Weitere Informationen finden Sie unter 'Abschneiden von Transaktionsprotokollen (S. 228)'
2. Bei Microsoft Exchange Server, unter Verwendung des dedizierten Agenten für Exchange.
3. Für Microsoft SQL Server, unter Verwendung des Agenten für SQL.

Applikationsspezifische Empfehlungen

Siehe 'Optimale Vorgehensweisen beim Backup von Anwendungsservern (S. 232)'.

11.1.1 Datenbankdateien suchen

Dieser Abschnitt beschreibt, wie Sie Anwendungsdatenbankdateien finden können.

Wir empfehlen, dass Sie die Datenbankdatei-Pfade ermitteln und diese dann an einem sicheren Platz speichern. Sie sparen sich damit Zeit und Aufwand, wenn Sie die Anwendungsdaten wiederherstellen wollen.

11.1.1.1 SQL Server-Datenbankdateien

SQL Server-Datenbanken haben drei Arten von Dateien:

- Primäre Datendateien – haben standardmäßig die Erweiterung **.mdf**. Jede Datenbank hat eine primäre Datendatei.
- Sekundäre Datendateien – haben standardmäßig die Erweiterung **.ndf**. Sekundäre Datendateien sind optional. Manche Datenbanken haben überhaupt keine, andere Datenbanken können dagegen mehrere sekundäre Datendateien haben.
- Protokolldateien – haben standardmäßig die Erweiterung **.ldf**. Jede Datenbank hat wenigstens eine Protokolldatei.

Stellen Sie sicher, dass alle Volumes, die irgendwelche der oberen Dateien enthalten, in das Backup aufgenommen werden. Falls Ihre Datenbanken beispielsweise im Verzeichnis 'C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data\' vorliegen und die Protokolldateien aber im Verzeichnis 'F:\TLs\', dann müssen Sie beide Volumes (C:\ und F:\) im Backup sichern.

Die Pfade zu allen Datenbankdateien einer Instanz per Transact-SQL bestimmen

Das folgende Transact-SQL-Skript kann 'wie vorliegend' verwendet werden, um die Pfade zu allen Datenbankdateien einer Instanz zu ermitteln.

```
Create Table ##temp
(
    DatabaseName sysname,
    Name sysname,
    physical_name nvarchar(500),
    size decimal (18,2),
    FreeSpace decimal (18,2)
)
Exec sp_msforeachdb '
Use [?];
Insert Into ##temp (DatabaseName, Name, physical_name, Size, FreeSpace)
    Select DB_NAME() AS [DatabaseName], Name,  physical_name,
    Cast(Cast(Round(cast(size as decimal) * 8.0/1024.0,2) as decimal(18,2)) as
nvarchar) Size,
    Cast(Cast(Round(cast(size as decimal) * 8.0/1024.0,2) as decimal(18,2)) -
        Cast(FILEPROPERTY(name, ''SpaceUsed'') * 8.0/1024.0 as decimal(18,2)) as
nvarchar) As FreeSpace
    From sys.database_files'
Select * From ##temp
drop table ##temp
```

Die Speicherorte von Datenbankdateien per SQL Server Management Studio bestimmen

Standardspeicherorte

SQL Server-Datenbankdateien liegen in ihren Standardspeicherorten vor, sofern Sie die Pfade nicht manuell angepasst haben. So ermitteln Sie die Standardpfade von Datenbankdateien:

1. Führen Sie Microsoft SQL Server Management Studio aus und verbinden Sie sich mit der benötigten Instanz.
2. Klicken Sie mit der rechten Maustaste auf den Instanznamen und wählen Sie **Eigenschaften**.
3. Öffnen Sie die Seite **Datenbankeinstellungen** überprüfen Sie die im Bereich **Standardspeicherorte für Datenbank** angegebenen Pfade.

Benutzerdefinierte Speicherorte

Sollten die Speicherorte der SQL Server-Datenbankdateien angepasst worden sein, dann gehen Sie folgendermaßen vor:

1. Erweitern Sie im Microsoft SQL Server Management Studio die benötigte Instanz.
2. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**. Darauf öffnet sich das Dialogfenster **Datenbankeigenschaften**.
3. Klicken Sie im Fensterbereich **Seite auswählen** auf **Dateien** und überprüfen Sie die im Bereich **Datenbankdateien** angegebenen Pfade.

11.1.1.2 Exchange-Server-Datenbankdateien

Exchange-Datenbanken haben drei Arten von Dateien:

- **Datenbankdatei (.edb)**

  Enthält Nachrichtenköpfe, Nachrichtentext und Standardanhänge.

  Eine Exchange 2003/2007-Datenbank verwendet zwei Dateien: .edb für Textdaten und .stm für MIME-Daten.
- **Transaktionsprotokolldateien (.log)**

Enthält den Verlauf von an der Datenbank durchgeführten Änderungen. Erst nachdem eine Änderung sicher protokolliert wurde, wird diese dann auch in die Datenbankdatei geschrieben. Dieser Ansatz garantiert eine zuverlässige Wiederherstellung der Datenbank zu einem konsistenten Zustand, für den Fall, dass es zu einer plötzlichen Datenbankstörung kommt.

Die Größe jeder Protokolldatei beträgt 1024 KB (oder 5120 KB bei Exchange 2003) Sobald eine aktive Protokolldatei voll ist, schließt Exchange diese und erstellt eine neue Protokolldatei.

- **Prüfpunktdatei (.chk)**

  Verfolgt, wie weit Exchange damit fortgeschritten ist, protokollierte Informationen in die Datenbankdatei zu schreiben.

Gehen Sie folgendermaßen vor, um die Datenbankdatei- und Protokolldatei-Pfade herauszufinden.

Exchange 2010

Führen Sie mit der Exchange-Verwaltungsshell folgende Befehle aus:

```
Get-MailboxDatabase | Format-List -Property Name, EdbFilePath, LogFolderPath
```

Exchange 2007

Führen Sie mit der Exchange-Verwaltungsshell folgende Befehle aus:

- So rufen Sie die Datenbank-Pfade ab:

  ```
  Get-MailboxDatabase | Format-List -Property Name, EdbFilePath, StorageGroup
  ```

- So rufen Sie die Protokolldatei-Pfade ab:

  ```
  Get-MailboxDatabase | ForEach { Get-StorageGroup $_.StorageGroupName | Format-List
  -Property Name, LogFolderPath }
  ```

Exchange 2003

1. Starten Sie den Exchange-System-Manager.
2. Klicken Sie auf **Administrative Gruppen**.

   ***Anmerkung**: Sollten die administrativen Gruppen nicht erscheinen, dann sind sie möglicherweise nicht angeschaltet. Klicken Sie mit der rechten Maustaste zum Anschalten der administrativen Gruppen auf **Exchange-Organisation** und dann auf **Eigenschaften**. Klicken Sie, um das Kontrollkästchen 'Administrative Gruppen anzeigen' zu aktivieren.*

3. Gehen Sie folgendermaßen vor, um den Transaktionsprotokoll-Speicherort zu ermitteln:
   a. Klicken Sie mit der rechten Maustaste auf die Speichergruppe und wählen Sie **Eigenschaften**.
   b. Auf der Registerkarte **Allgemein** wird der Transaktionsprotokoll-Speicherort angezeigt.
4. Gehen Sie folgendermaßen vor, um den Datenbankdatei-Speicherort (für *.edb-Dateien) zu ermitteln:
   a. Erweitern Sie die benötigte Speichergruppe
   b. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**.
   c. Sie sehen in der Registerkarte **Datenbank** den Speicherort der Datenbankdatei und der Datenbank-Streamingdatei.

11.1.1.3 Active Directory-Datenbankdateien

Eine Active Directory-Datenbank besteht aus folgenden Dateien:

1. **NTDS.dit** (Datenbankdatei)
2. **Edb.chk** (Prüfpunktdatei)

3. **Edb*.log** (Transaktionsprotokolle)
4. **Res1.log** und **Res2.log** (zwei Reserveprotokolldateien)

Die Dateien befinden sich typischerweise im Ordner **%systemroot%\NTDS** (beispielsweise C:\Windows\NTDS) eines Domain Controllers. Ihr Speicherort ist jedoch konfigurierbar. Die Datenbankdateien und die Transaktionsprotokolle können auf unterschiedlichen Volumes gespeichert werden. Stellen Sie sicher, dass beide Volume in das Backup aufgenommen werden.

Um den aktuellen Speicherort der Datenbankdateien und Transaktionsprotokolle bestimmen zu können, müssen Sie die Werte **DSA Database file** und **Database log files path** in folgenden Registry-Schlüsseln überprüfen:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

11.1.1.4 SharePoint-Datenbankdateien

SharePoint speichert Inhalte, Hilfsdaten der SharePoint-Dienste und die Farmkonfiguration in Microsoft SQL Server-Datenbanken.

So finden Sie Datenbankdateien in SharePoint 2010 (oder höher)

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Upgrade und Migration** –> **Datenbankstatus überprüfen**. Ihnen werden die SQL-Instanz und die Datenbanknamen für alle Datenbanken angezeigt.
3. Verwenden Sie Microsoft SQL Server Management Studio, um die Dateien der benötigten Datenbank zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 224).

So finden Sie Inhaltsdatenbankdateien in SharePoint 2007

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Anwendungsmanagement** –> **Inhaltsdatenbanken**.
3. Wählen Sie eine Webapplikation.
4. Wählen Sie eine Datenbank. Sie sehen in der geöffneten Seite den Datenbankserver und den Datenbanknamen. Notieren Sie diese oder kopieren Sie die Information in eine Textdatei.
5. Wiederholen Sie Schritt 4 für andere Datenbanken der Webapplikation.
6. Wiederholen Sie die Schritte 3-5 für andere Webapplikationen.
7. Verwenden Sie Microsoft SQL Server Management Studio, um die Datenbankdateien zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 224).

So finden Sie Konfigurations- oder Dienstdatenbankdateien in SharePoint 2007

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Anwendungsmanagement** –> **Gemeinsame Dienste dieser Farm erstellen oder konfigurieren**.
3. Klicken Sie mit der rechten Maustaste auf einen Anbieter für gemeinsame Dienste (Shared Services Provider) und wählen Sie **Eigenschaften bearbeiten**. Sie sehen in der geöffneten Seite den Datenbankserver und den Datenbanknamen. Notieren Sie diese oder kopieren Sie die Information in eine Textdatei.
4. Wiederholen Sie Schritt 3 für andere Anbieter für gemeinsame Dienste.
5. Verwenden Sie Microsoft SQL Server Management Studio, um die Datenbankdateien zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 224).

11.1.2 Abschneiden von Transaktionsprotokollen

Dieser Abschnitt beschreibt, wie Sie Transaktionsprotokolle abschneiden können, wenn Sie Microsoft Exchange Server und Microsoft SQL Server mithilfe von Laufwerk-Backups schützen.

Die Empfehlungen für SQL Server gelten auch für SQL Server, die in einer Microsoft SharePoint-Farm enthalten sind. Active Directory-Datenbanken verwenden normalerweise Umlaufprotokollierung, daher benötigen Sie kein Abschneiden von Transaktionsprotokollen.

11.1.2.1 Abschneiden des Transkationsprotokolls und Verkleinern der Protokolldatei für SQL Server

Acronis Backup schneidet Transaktionsprotokolle nach Erstellung eines Laufwerk-Backups nicht ab. Falls Sie nicht die systemeigene Backup-Engine des Microsoft SQL Servers verwenden (oder die Backup-Lösung eines anderen Drittherstellers, die Transaktionsprotokolle automatisch verwaltet), dann können Sie die Protokolle mit folgenden Methoden verwalten.

- **Abschneiden des Transaktionsprotokolls**. Das Protokollabschneiden macht inaktive virtuelle Protokolldateien (die nur inaktive Protokolldatensätze enthalten) frei zur Wiederverwendung durch neue Protokolldatensätze. Abschneiden kann eine physikalische Protokolldatei daran hindern zu wachsen, aber dadurch wird nicht ihre Größe reduziert.

  Weitere Informationen über das Abschneiden finden Sie in folgendem Artikel: http://technet.microsoft.com/de-de/library/ms189085(v=sql.105)
- **Verkleinern der Protokolldatei**. Das Verkeinern einer Protokolldatei reduziert die physikalische Größe einer Protokolldatei, indem inaktive virtuelle Protokolldateien entfernt werden. Das Verkleinern ist am wirksamsten nach einer Protokollabschneidung.

  Weitere Informationen über das Verkleinern finden Sie in folgendem Artikel: http://technet.microsoft.com/de-de/library/ms178037(v=sql.105)

Protokollabschneidung durch SQL Server Management Studio

Wenn Sie eine Datenbank auf das einfache Wiederherstellungsmodell (Simple Recovery Model) umschalten, werden die Transaktionsprotokolle automatisch abgeschnitten.

1. So schalten Sie die Datenbank auf das einfache Wiederherstellungsmodell um:
   a. Führen Sie Microsoft SQL Server Management Studio aus und verbinden Sie sich mit der Instanz.
   b. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**. Darauf öffnet sich das Dialogfenster **Datenbankeigenschaften**.
   c. Klicken Sie im Fensterbereich **Seite auswählen** auf **Optionen**.
   d. Wählen Sie im Listenfeld **Wiederherstellungsmodell** das Modell **Einfach**.
2. Die Transaktionsprotokolldateien werden automatisch abgeschnitten.
3. Schalten Sie die Datenbank, auf gleiche Art wie in Schritt 1, zurück zum vollständigen oder massenprotokollierten Wiederherstellungsmodell.

Protokollabschneidung und -verkleinerung automatisieren

Sie können die obere Prozedur des Abschneidens mit einem Skript automatisieren und (optional) auch das Protokolldatei-Verkleinern hinzufügen. Falls Sie das Skript zu den 'Nach-Backup'-Befehlen (S. 104) hinzufügen, werden die Protokolle direkt nach einem Backup abgeschnitten und verkleinert. Bei dieser Methode wird angenommen, dass Sie über Kenntnisse zur Erstellung/Nutzung von Transact-SQL-Skripten verfügen und sich mit dem Utility **`sqlcmd`** auskennen.

Weitere Informationen über Transact-SQL und **sqlcmd** finden Sie in folgenden Artikeln:

- Transact-SQL verwenden: http://technet.microsoft.com/de-de/library/ms189826(v=sql.90)
- Das Utility **sqlcmd** verwenden: http://technet.microsoft.com/de-de/library/ms170572(SQL.90).aspx

So automatisieren Sie das Abschneiden und Verkleinern des Transaktionsprotokolls für eine SQL-Instanz

1. Erstellen Sie durch Verwendung des folgenden Templates ein Skript, welches die Protokolldateien für die Datenbanken der folgenden Instanz abschneidet und verkleinert:

   ```
   USE database_name
   ALTER DATABASE database_name SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(logfile_name);
   ALTER DATABASE database_name SET RECOVERY FULL;
   ```

   Im letzten String hängt der Wert **SET RECOVERY** vom ursprünglichen Wiederherstellungsmodell der bestimmten Datenbank ab und kann **FULL** (vollständig) oder **BULK_LOGGED** (massenprotokolliert) sein.

   Beispiel für eine Instanz, die zwei Datenbanken (TestDB1 und TestDB2) hat:

   ```
   USE TestDB1;
   ALTER DATABASE TestDB1 SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(TestDB1_log);
   ALTER DATABASE TestDB1 SET RECOVERY FULL;

   USE TestDB2;
   ALTER DATABASE TestDB2 SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(TestDB2_log);
   ALTER DATABASE TestDB2 SET RECOVERY BULK_LOGGED;
   ```

2. Fügen Sie den nachfolgenden **sqlcmd**-Befehl dem 'Nach-Backup'-Befehl (S. 104) hinzu:

   ```
   sqlcmd -S myServer\instanceName -i C:\myScript.sql
   ```

   Dabei ist:

   - `myServer` – der Name des Servers
   - `instanceName` – der Name der Instanz
   - `C:\myScript.sql` – der Pfad zur in Schritt 1 erstellten Skriptdatei.

So automatisieren Sie das Abschneiden und Verkleinern des Transaktionsprotokolls für mehrere SQL-Instanzen

Falls Sie mehr als eine Instanz auf der Maschine haben und Sie die obere Prozedur auf diese Instanzen anwenden wollen, dann gehen Sie folgendermaßen vor.

1. Erstellen Sie eine separate Skriptdatei für jede Instanz (z. B. C:\script1.sql und C:\script2.sql).
2. Erstellen Sie eine Batchdatei (z.B. C:\truncate.bat), welche die Befehle für die korrespondierende Instanz enthält:

   ```
   sqlcmd -S myServer\instance1 -i C:\script1.sql
   sqlcmd -S myServer\instance2 -i C:\script2.sql
   ```

3. Spezifizieren Sie bei 'Nach-Backup-Befehl' den Pfad zu dieser Batchdatei.

11.1.2.2 Abschneiden des Transaktionsprotokolls für Exchange-Server

Über Microsoft Exchange-Server-Protokolle

Bevor eine Transaktion auf eine Datenbankdatei ausgeführt wird, protokolliert Exchange diese in eine Transaktionsprotokolldatei. Um zu verfolgen, welche der protokollierten Transaktionen auf die

Datenbank angewendet wurden, verwendet Exchange Prüfpunktdateien. Sobald die Transaktionen auf die Datenbank angewendet und per Prüfpunktdateien verfolgt wurden, werden die Protokolldateien nicht mehr länger von der Datenbank benötigt.

Werden die Protokolldateien nicht gelöscht, können diese möglicherweise den kompletten verfügbaren Speicherplatz belegen – und die Exchange-Datenbanken werden offline genommen, bis die Protokolldateien vom Laufwerk entfernt wurden. Die Verwendung von Umlaufprotokollierung ist nicht die bewährteste Methode für eine Produktionsumgebung. Bei aktivierter Umlaufprotokollierung überschreibt Exchange die erste Protokolldatei, nachdem deren Daten auf die Datenbank angewendet wurden – wodurch Sie nur Daten bis zum letzten Backup wiederherstellen können.

Wir empfehlen, dass Sie die Protokolldateien nach dem Backup eines Exchange-Servers löschen, weil Protokolldateien zusammen mit anderen Dateien gesichert werden. Sie können die Datenbank nach einer Wiederherstellung daher vorwärts und rückwärts 'rollen'.

Weitere Informationen über die Transaktionsprotokollierung finden Sie unter http://technet.microsoft.com/de-de/library/bb331958.aspx .

Protokollabschneidung unter Verwendung der Option VSS-Voll-Backup aktivieren

Die einfachste Methode der Protokollabschneidung ist die Verwendung der Backup-Option **VSS-Voll-Backup aktivieren** (S. 109) (**Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup** –> **Volume Shadow Copy Service** –> **VSS-Voll-Backup aktivieren**). Sie wird in den meisten Fällen empfohlen.

Sollte eine Aktivierung dieser Option unerwünscht sein (weil Sie beispielsweise die Protokolle einer anderen VSS-kompatiblen Anwendung bewahren müssen), dann folgen Sie den unteren Empfehlungen.

Abschneiden von Offline-Datenbanken protokollieren

Nach einem normalen Herunterfahren wird der Datenbankzustand als konsistent angesehen und die Datenbankdateien sind eigenständig (self-contained). Das bedeutet, dass Sie alle Protokolldateien der Datenbank oder Speichergruppe löschen können.

So löschen Sie Transaktionsprotokolldateien:

1. Trennen Sie die Datenbank (bei Exchange 2010) oder alle Datenbanken der Speichergruppe (bei Exchange 2003/2007). Zu weiteren Informationen, siehe:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/bb123903
   - Exchange 2007: http://technet.microsoft.com/de-de/library/bb124936(v=exchg.80)
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa996179(v=exchg.65)
2. Löschen Sie alle Protokolldateien der Datenbank oder der Speichergruppe.
3. Mounten Sie die getrennte(n) Datenbank oder Datenbanken.

   Zu weiteren Informationen, siehe:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/bb123587.aspx
   - Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=exchg.80).aspx
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa995829(v=exchg.65)

Abschneiden von Online-Datenbanken protokollieren

Diese Methode ist gut für Datenbanken, die permanent verwendet werden und daher nicht getrennt werden können. Wenn sich eine Datenbank in Verwendung befindet, können Sie nur solche

Transaktionsprotokolldateien sichern löschen, deren Daten auf die Datenbank angewendet wurden. Löschen Sie keine Protokolldateien, deren Daten nicht auf die Datenbank angewendet wurden; sie sind essentiell, um die Datenbank-Konsistenz bei unerwartetem Herunterfahren wiederherstellen zu können.

So löschen Sie angewendete Transaktionsprotokolle

1. Bestimmen Sie mit dem Tool **`Eseutil`**, welche Protokolle auf die Datenbank angewendet wurden:
   a. Führen Sie den Befehl **`eseutil /mk`** `<Pfad zur Prüfpunktdatei>` aus, wobei `<Pfad zur Prüfpunktdatei>` der Pfad zu der Prüfpunktdatei für die benötigte Datenbank oder Speichergruppe ist.
   b. Überprüfen Sie das Feld **`Checkpoint`** in der Anzeige. Sie sollten etwas sehen, das etwa so aussieht:

   ```
   CheckPoint: (0x60B, 7DF, 1C9)
   ```

   Die erste Zahl 0x60B ist die hexadezimale Protokollgenerierungsnummer der aktuellen Protokolldatei. Das bedeutet, dass alle Protokolldateien mit kleineren Zahlen auf die Datenbank angewendet wurden.
2. Löschen Sie alle Protokolldateien, deren Zahlen kleiner sind als die Zahl der aktuellen Protokolldatei. Sie können beispielsweise die Dateien Enn0000060A.log, Enn00000609.log (und niedrigere Dateien) sicher löschen.

Abschneiden nach einem Backup protokollieren

Sie können die obere Prozedur des Abschneidens mit einem Skript automatisieren. Falls Sie das Skript zu den 'Nach-Backup'-Befehlen (S. 104) hinzufügen, werden die Protokolle direkt nach einem Backup abgeschnitten.

Bei dieser Methode wird angenommen, dass Sie über Kenntnisse zur Erstellung/Nutzung von Skripten verfügen und sich mit dem Befehlszeilenwerkzeug von Acronis Backup auskennen (**`acrocmd`**). Weitere Informationen zu **`acrocmd`** finden Sie in der Befehlszeilen-Referenz.

Das Skript sollte folgende Schritte enthalten:

1. Mounten Sie die Volumes, die die benötigten Datenbankdateien enthalten, durch Verwendung des Befehls **`mount`**.

   Template:

   ```
   acrocmd mount --loc=<Pfad> --credentials=<Benutzername>,<password>
   --arc=<Archivname> --volume=<Volume-Nummern> --letter=<Laufwerksbuchstaben>
   ```

   Beispiel:

   ```
   acrocmd mount --loc=\\bkpsrv\backups --credentials=user1,pass1 --arc=my_arc
   --volume=1-1 --letter=Z
   ```

2. Bestimmen Sie in den gemounteten Volumes mit dem Tool **`Eseutil`**, welche Protokolle auf die Datenbank angewendet wurden. Diese Prozedur ist im Schritt 1 des oberen Abschnitts 'Abschneiden von Online-Datenbanken protokollieren' beschrieben.
3. Löschen Sie in der entsprechenden Online-Datenbank oder Speichergruppe alle Protokolldateien, deren Zahlen niedriger sind, als die Zahl der aktuellen Protokolldatei im Backup.
4. Trennen Sie die gemounteten Volumes durch Verwendung des Befehls **`umount`**.

11.1.3 Optimale Vorgehensweisen beim Backup von Anwendungsservern

11.1.3.1 Exchange-Server-Backup

Falls Sie nicht Microsoft Exchange Server 2010 SP2 (oder höher) verwenden, wird empfohlen, dass Sie die Konsistenz von Exchange-Datenbankdateien regelmäßig überprüfen.

In Exchange wird die Konsistenzprüfung mit dem Tool bzw. Befehl **`Eseutil /K`** durchgeführt. Dabei wird die Seitenebenenintegrität (Page-Level Integrity) von allen Exchange-Datenbanken und die Prüfsummen aller Datenbankseiten und Protokolldateien verifiziert. Der Überprüfungsvorgang kann zeitaufwendig sein. Weitere Informationen über die Verwendung von **`Eseutil /K`** finden Sie unter: http://technet.microsoft.com/de-de/library/bb123956(v=exchg.80) .

Sie können die Konsistenzprüfung vor oder nach einem Backup durchführen.

- **Vor einem Backup**. Das gewährleistet, dass Sie keine beschädigten Echange-Datenbankdateien per Backup sichern.
  a. Trennen Sie die Datenbanken.
  b. Führen Sie **`Eseutil /K`** aus und überprüfen Sie die Ergebnisse der Verifizierung.
  c. Sollten die Datenbanken konsistent sein, dann mounten Sie sie erneut und führen Sie das Backup aus. Reparieren Sie anderenfalls die beschädigten Datenbanken.

  Weitere Informationen über Mounten und Trennen (Dismounten) von Datenbanken finden Sie im Abschnitt 'Abschneiden des Transaktionsprotokolls für Exchange-Server (S. 229)'.
- **Nach einem Backup**. Der Vorteil dieser Methode ist, dass Sie keine permanent verwendeten Datenbanken trennen müssen. Die Konsistenzprüfung im Backup ist jedoch viel langsamer als die Konsistenzprüfung von auf dem Laufwerk liegenden Datenbanken.

  Mounten (S. 181) Sie die Volumes (welche die benötigten Datenbankdateien enthalten) von dem Laufwerk-Backup im 'Nur Lesen'-Modus und führen Sie dann **`Eseutil /K`** aus.

  Sollte eine Prüfsummen-Inkonsistenz oder ein beschädigter Datei-Header gefunden werden, dann reparieren Sie die beschädigten Datenbanken und führen Sie das Backup erneut aus.

***Tipp:** Acronis hat ein dediziertes Produkt zum Backup von Microsoft Exchange im Angebot – Acronis Backup Advanced für Exchange. Wenn Sie dieses Produkt verwenden, überprüft der Agent für Exchange automatisch die Konsistenz von zu sichernden Datenbanken und überspringt Datenbanken mit Prüfsummen-Inkonsistenz oder beschädigtem Datei-Header. Im Gegensatz zu diesem Agenten verifiziert **`Eseutil /K`** die Seiten aller Exchange-Datenbanken, die auf dem Server vorhanden sind.*

11.1.3.2 Active Directory-Backup

Die Active Directory-Dienste verwenden eine Datenbank, die sich auf dem Dateisystem eines Domain-Controllers befindet. Falls die Domain zwei oder mehr Domain-Controller hat, werden die in der Datenbank gespeicherten Informationen kontinuierlich zwischen den Controllern repliziert.

Zu sichernde Volumes

Erstellen Sie Backups folgender Volumes eines Domain-Controllers, um ein Active Directory zu sichern:

- Das System-Volume und das Boot-Volume
- Die Volumes, auf denen sich die Active Directory-Datenbank und Transaktionsprotokolle (S. 226) befinden

- Das Volume mit dem Ordner SYSVOL. Der Standardort für dieses Verzeichnis ist **%SystemRoot%\SYSVOL**. Untersuchen Sie, um den aktuellen Speicherort dieses Ordners zu ermitteln, den **Sysvol**-Wert in folgendem Registry-Schlüssel:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
  ```

Weitere Überlegungen zum Backup

Stellen Sie bei der Einrichtung und Durchführung von Active Directory-Backups sicher, dass:

- Die Häufigkeit der Backup-Durchführung ist **mindestens monatlich.** Sollte Ihre Domain nur einen Domain-Controller haben, dann empfehlen wir eine mindestens tägliche Backup-Erstellung.
- Ihr aktuellstes Backup ist **nicht älter als die Hälfte der Tombstone-Lebensdauer.** Abhängig vom Betriebssystem, auf der Ihre Domain erstellt wurde, beträgt die vorgegebene Tombstone-Lebensdauer 60 oder 180 Tage. Es ist nicht wichtig, ob das letzte Backup vollständig oder inkrementell ist, denn Sie können erfolgreiche Wiederherstellungen von beiden ausführen.
- Sie können ein **zusätzliches Backup bei einem der folgenden Ereignisse** erstellen:
  - Die Active Directory-Datenbank und/oder Transaktionsprotokolle wurden zu einem anderen Speicherort verschoben.
  - Das Betriebssystem auf dem Domain-Controller wurde per Upgrade aktualisiert oder es wurde ein Service Pack installiert.
  - Es wurde ein Hotfix installiert, welches die Active Directory-Datenbank ändert.
  - Die Tombstone-Lebensdauer wurde administrativ geändert.

  Der Grund für dieses zusätzliche Backup ist, dass eine erfolgreiche Wiederherstellung des Active Directory von früheren Backups evtl. nicht mehr möglich ist.

11.1.3.3 SharePoint-Daten-Backup

Eine Microsoft SharePoint-Farm besteht aus Front-End-Webservern und Microsoft SQL Servern.

Ein Front-End-Webserver ist ein Host, auf dem SharePoint-Dienste laufen. Einige Front-End-Webserver können zueinander identisch sein (beispielswiese Front-End-Webserver, die einen Webserver ausführen). Sie müssen keine identischen Front-End-Webserver per Backup sichern, sondern nur individuelle.

Sie müssen, um SharePoint-Datenbanken sichern zu können, alle Microsoft SQL Servers und alle individuellen, zu der Farm gehörenden Front-End-Webserver per Backup sichern. Das Backup sollte mit *derselben Planung* durchgeführt werden. Das ist notwendig, weil die Konfigurationsdatenbank mit anderen Datenbanken synchronisiert werden muss. Falls beispielsweise die Inhaltsdatenbank Daten über eine Website enthält, während das letzte Backup der Konfigurationsdatenbank dies nicht tut, dann wird die Website nach Wiederherstellung der Konfigurationsdatenbank verwaist sein.

Falls Sie Acronis Backup Advanced haben, ist der einfachste Weg, Backups einer SharePoint-Farm zu erstellen, entweder einen zentralen Backup-Plan zu erstellen (wie im Abschnitt 'Erstellung eines zentralen Backup-Plans' beschrieben) – oder die Funktion **Backup jetzt** zu verwenden (wie im Abschnitt 'Backup jetzt' beschrieben). Bei Acronis Backup müssen Sie dieselbe Planung bei Erstellung eines Backup-Plans (S. 38) für jeden zur Farm gehörenden Server spezifizieren.

11.2 Wiederherstellung von SQL Server-Daten

Bei einem Desaster können Sie einen kompletten SQL Server dadurch wiederherstellen, dass Sie all seine Laufwerke von einem Laufwerk-Backup wiederherstellen. Sollten Sie den im Abschnitt 'Backup eines Anwendungsservers (S. 222)' aufgeführten Empfehlungen gefolgt sein, dann sind alle SQL

Server-Dienste funktionell und laufen, ohne dass weitere Aktionen notwendig sind. Die Server-Daten werden auf das Stadium zurückgesetzt, die zum Zeitpunkt des Backups gehabt haben.

Falls Sie eine gesicherte Datenbank zurück in die Produktion bringen müssen, dann stellen Sie die Datenbankdateien aus einem Laufwerk-Backup wieder her. Weitere Details finden Sie unter 'Wiederherstellung von SQL Server-Datenbankdateien von einem Laufwerk-Backup (S. 234)'.

Sollten Sie nur einen temporären Zugriff auf die gesicherten Datenbanken benötigen (zur Datengewinnung oder Datenextraktion), dann mounten Sie ein Laufwerk-Backup und greifen Sie auf die erforderlichen Daten zu. Weitere Details finden Sie unter 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 235)'.

11.2.1 Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup

Dieser Abschnitt beschreibt, wie Sie SQL Server-Datenbanken von einem Laufwerk-Backup ausgehend wiederherstellen können.

Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'SQL Server-Datenbankdateien (S. 224)'.

So stellen Sie SQL Server-Datenbanken wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Aktion durchführen werden.
2. Gehen Sie zu dem Depot, welches das Laufwerk-Backup mit den SQL Server-Datenbankdateien enthält.
3. Klicken Sie auf Registerkarte **Datenanzeige**. Klicken Sie in der Liste **Anzeigen** auf **Ordner/Dateien**.
4. Wählen Sie die benötigten SQL Server-Datenbankdateien und klicken Sie auf **Recovery**. Die Daten werden standardmäßig auf den Zustand des letzten Backups zurückgesetzt. Verwenden Sie die Liste **Versionen**, falls Sie einen anderen Zeitpunkt wählen wollen, auf den die Daten zurückgesetzt werden sollen.
5. Auf der Recovery-Seite, unter dem Bereich **Recovery-Quelle**:
   a. Wählen Sie bei **Datenpfade** den Punkt **Benutzerdefiniert**.
   b. Spezifizieren Sie bei **Durchsuchen** einen Ordner, wohin die Dateien wiederhergestellt werden sollen.

      ***Anmerkung**: Wir empfehlen, dass Sie die SQL Server-Datenbankdateien zu einem lokalen Ordner des SQL Servers wiederherstellen, da alle SQL Server-Versionen vor SQL Server 2012 keine Datenbanken unterstützen, die auf Netzwerkfreigaben liegen.*

   c. Belassen Sie die übrigen Einstellungen wie vorliegend und klicken Sie dann auf **OK**, um dem Recovery-Task fortzufahren.
6. Fügen Sie die Datenbank nach Abschluss der Wiederherstellung so an, wie im Abschnitt 'SQL Server-Datenbanken anfügen (S. 235)' beschrieben.

   Details: Sollte Sie aus irgendeinem Grund nicht alle SQL Server-Datenbankdateien wiederhergestellt haben, dann können Sie die Datenbank nicht anfügen. Das Microsoft SQL Server Management Studio informiert Sie jedoch über alle Pfade und Namen der fehlenden Dateien und hilft Ihnen dabei zu identifizieren, aus welchen konkreten Dateien die Datenbank besteht.

11.2.2 Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus

Falls Sie zur Datengewinnung oder aus anderen, kurzfristigen Gründen auf die SQL Server-Datenbanken zugreifen wollen, können Sie statt einer Wiederherstellung die Aktion **Image mounten** verwenden. Mounten Sie einfach die entsprechenden Volumes (die die benötigten Datenbankdateien enthalten) von einem Laufwerk-Backup (Image) im 'Lese/Schreib'-Modus und Sie können Datenbanken anfügen, Datenbankdateien ändern und mit diesen arbeiten, als würden Sie sich auf einem physikalischen Laufwerk befinden.

Sie können Volumes mounten, falls das Laufwerk-Backup in einem lokalen Ordner (ausgenommen optische Medien wie CDs, DVDs oder Blu-ray-Medien), in der Acronis Secure Zone oder auf einer Netzwerkfreigabe gespeichert vorliegt.

Anfügen von Datenbanken an einen SQL Server, die in einem Laufwerk-Backup enthalten sind

1. Verbinden Sie die Konsole mit dem SQL Server, auf dem der Agent für Windows installiert ist.
2. Wählen Sie im Hauptmenü die Befehle **Aktionen** –> **Image mounten**.
3. Wählen Sie im Bereich **Zu mountendes Image** das Quellarchiv und spezifizieren Sie das Backup.
4. Im Bereich **Mount-Einstellungen**:
   a. Wählen Sie bei **Mounten für** die Option **Alle Benutzer dieser Maschine**.
   b. Wählen Sie ein oder mehrere Volumes, welche die SQL Server-Datenbankdateien enthalten. Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'SQL Server-Datenbankdateien (S. 224)'.
   c. Wählen Sie den Zugriffsmodus **Lesen/Schreiben**.
   d. Spezifizieren Sie Laufwerksbuchstaben, die den gemounteten Volumes zugewiesen werden.
5. Verwenden Sie nach dem Mounten der Volumes die Anweisungen aus dem Abschnitt 'SQL Server-Datenbanken anfügen (S. 235)', um die Datenbanken direkt von den gemounteten Volumes aus anzufügen.
6. Führen Sie die gewünschten Aktionen mit den neu angefügten Datenbanken durch.
7. Trennen Sie die Datenbanken wieder von der Instanz, nachdem Sie die gewünschten Aktionen abgeschlossen haben, indem Sie Microsoft SQL Server Management Studio verwenden. Klicken Sie dazu mit der rechten Maustaste auf die Datenbank und wählen Sie **Aufgaben** –> **Trennen**.
8. Trennen Sie die gemounteten Volumes:
   a. Wählen Sie im Hauptmenü die Befehle **Navigation** –> **Gemountete Images**.
   b. Wählen Sie das Image und klicken Sie auf **Trennen**.

   Details: Acronis Backup erstellt beim Mounten eines Images im 'Lese/Schreib'-Modus ein neues inkrementelles Backup. Wir empfehlen, dieses inkrementelle Backup zu löschen.

11.2.3 SQL Server-Datenbanken anfügen

Dieser Abschnitt beschreibt, wie Sie eine Datenbank im SQL Server mithilfe des SQL Server Management Studios anfügen können. Es kann immer nur eine Datenbank gleichzeitig angefügt werden.

Das Anfügen einer Datenbank erfordert eine der folgenden Berechtigungen: **Datenbank erstellen**, **Beliebige Datenbank erstellen** oder **Beliebige Datenbank ändern**. Normalerweise verfügt auf der Instanz die Rolle **SysAdmin** über diese Berechtigungen.

So fügen Sie eine Datenbank an

1. Führen Sie Microsoft SQL Server Management Studio aus.
2. Verbinden Sie sich mit der benötigten SQL Server-Instanz und erweitern Sie dann die Instanz.
3. Klicken Sie mit der rechten Maustaste auf **Datenbanken** und klicken Sie dann auf **Anfügen**.
4. Klicken Sie auf **Hinzufügen**.
5. Lokalisieren und Wählen Sie im Dialogfenster **Datenbankdateien suchen** die .mdf-Datei der Datenbank.
6. Stellen Sie im Bereich **Datenbankdetails** sicher, dass die restlichen Datenbankdateien (.ndf- und .ldf-Dateien) gefunden werden.

   Details: SQL Server-Datenbankdateien werden möglicherweise nicht automatisch gefunden, falls:

   - Sie sich nicht am Standardspeicherort befinden – oder sie nicht im selben Ordner wie die primäre Datenbankdatei (.mdf) sind.Lösung: Spezifizieren Sie den Pfad zu den benötigten Dateien manuell in der Spalte **Aktueller Dateipfad**.
   - Sie haben einen unvollständigen Satz an Dateien wiederhergestellt, der die Datenbank bildet. Lösung: Stellen Sie die fehlenden SQL Server-Datenbankdateien aus dem Backup wieder her.
7. Klicken Sie, wenn alle Dateien gefunden sind, auf **OK**.

11.3 Wiederherstellung von Exchange-Server-Daten

Bei einem Desaster können Sie einen kompletten Exchange-Server dadurch wiederherstellen, dass Sie all seine Laufwerke von einem Laufwerk-Backup wiederherstellen. Sollten Sie den im Abschnitt 'Backup eines Anwendungsservers (S. 222)' aufgeführten Empfehlungen gefolgt sein, dann sind alle Exchange-Server-Dienste funktionell und laufen, ohne dass weitere Aktionen notwendig sind. Die Server-Daten werden auf das Stadium zurückgesetzt, die zum Zeitpunkt des Backups gehabt haben.

Durch Verwendung von Acronis Backup können Sie Exchange-Datenbankdateien von einem Laufwerk-Backup wiederherstellen. Mounten Sie eine Datenbank, um Sie wieder online zu bringen. Weitere Details finden Sie unter 'Mounten von Exchange-Server-Datenbanken (S. 237)'.

Falls Sie eine granuläre Wiederherstellung einzelner Postfächer (oder von in diesen enthaltenen Elementen) durchführen müssen, dann mounten Sie die wiederhergestellte Datenbank entweder als Wiederherstellungsdatenbank (Recovery Database, RDB) bei Exchange 2010 – oder als Speichergruppe für die Wiederherstellung (Recovery Storage Group, RSG) bei Exchange 2003/2007. Weitere Details finden Sie im Abschnitt 'Granuläres Recovery von Postfächern (S. 237)'.

11.3.1 Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup

Dieser Abschnitt beschreibt die Verwendung von Acronis Backup zur Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup.

Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'Exchange-Server-Datenbankdateien (S. 225)'.

So stellen Sie Exchange-Server-Datenbanken wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Aktion durchführen werden.
2. Gehen Sie zu dem Depot, welches das Laufwerk-Backup mit den Exchange-Datendateien enthält.
3. Klicken Sie auf Registerkarte **Datenanzeige**. Klicken Sie in der Liste **Anzeigen** auf **Ordner/Dateien**.

4. Wählen Sie die benötigten Exchange-Datenbankdateien und klicken Sie auf **Recovery**. Die Daten werden standardmäßig auf den Zustand des letzten Backups zurückgesetzt. Verwenden Sie die Liste **Versionen**, falls Sie einen anderen Zeitpunkt wählen wollen, auf den die Daten zurückgesetzt werden sollen.
5. Auf der Recovery-Seite, unter dem Bereich **Recovery-Quelle**:
   a. Wählen Sie bei **Datenpfade** den Punkt **Benutzerdefiniert**.
   b. Spezifizieren Sie bei **Durchsuchen** einen Ordner, wohin die Datenbankdateien wiederhergestellt werden sollen.
6. Belassen Sie die übrigen Einstellungen wie vorliegend und klicken Sie dann auf **OK**, um dem Recovery-Task fortzufahren.

11.3.2 Mounten von Exchange-Server-Datenbanken

Sie können die Datenbanken nach Wiederherstellung der Datenbankdateien dadurch wieder online bringen, dass Sie sie mounten. Das Mounten wird mithilfe der Exchange-Verwaltungskonsole, dem Exchange-System-Manager oder der Exchange-Verwaltungsshell durchgeführt.

Die wiederhergestellte Datenbank wird sich im Stadium 'Dirty Shutdown' befinden. Eine Datenbank, die sich im Zustand 'Dirty Shutdown' befindet, kann vom System gemountet werden, falls sie zu ihrem ursprünglichen Speicherort wiederhergestellt wurde (vorausgesetzt, die Information über die ursprüngliche Datenbank ist im Active Directory vorhanden). Wenn Sie eine Datenbank zu einem anderen Speicherort wiederherstellen (beispielsweise eine neue Datenbank oder die Wiederherstellungsdatenbank), dann kann die Datenbank solange gemountet werden, bis Sie sie mithilfe des Befehls **`Eseutil /r <Enn>`** in das Stadium 'Clean Shutdown' bringen. **`<Enn>`** gibt das Protokolldatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen.

Das Konto, welches Sie zum Anfügen einer Datenbank verwenden, muss an eine Exchange-Server-Administratorrolle und an eine lokalen Administratorengruppe des Zielservers delegiert sein.

Weitere Details zum Mounten von Datenbanken finden Sie in folgenden Artikeln:

- Exchange 2010: http://technet.microsoft.com/de-de/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=EXCHG.80).aspx
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb124040.aspx

11.3.3 Granuläres Recovery von Postfächern

Eine RDB (RSG) ist eine spezielle, administrative Datenbank (Speichergruppe) im Exchange-Server. Sie ermöglicht Ihnen, Daten aus einer gemounteten Postfach-Datenbank zu extrahieren. Die extrahierten Daten können zu existierenden Postfächern kopiert bzw. mit diesen zusammengeführt werden, ohne Benutzerzugriffe auf aktuelle Daten zu stören.

Weitere Informationen über RDB und RSG finden Sie in folgenden Artikeln:

- Exchange 2010: http://technet.microsoft.com/de-de/library/dd876954
- Exchange 2007: http://technet.microsoft.com/de-de/library/bb124039(v=exchg.80)
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb123631(v=exchg.65)

So stellen Sie ein Postfach wieder her

1. Sollte keine RDB/RSG vorhanden sein, dann erstellen Sie diese, wie in folgenden Artikeln beschrieben:

- Exchange 2010: http://technet.microsoft.com/de-de/library/ee332321
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa997694(v=exchg.80)
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb124427(v=exchg.65)

2. Stellen Sie die Datenbankdateien in die RDB/RSG-Ordnerstruktur wieder her. Weitere Informationen über die Wiederherstellung von Datenbankdateien finden Sie im Abschnitt 'Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup (S. 236)'.
3. Mounten Sie die Wiederherstellungsdatenbank. Weitere Informationen über das Mounten von Datenbanken finden Sie im Abschnitt 'Mounten von Exchange-Server-Datenbanken (S. 237)'.
4. Fahren Sie wie in folgenden Artikeln beschrieben fort:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/ee332351
   - Exchange 2007: http://technet.microsoft.com/de-de/library/aa997694(v=exchg.80)
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa998109(v=exchg.65)

11.4 Active Directory-Daten wiederherstellen

Eine Active Directory-Wiederherstellung ist unterschiedlich, abhängig vom erforderlichen Wiederherstellungstyp.

Dieser Abschnitt betrachtet folgende Desaster-Szenarien:

- Ein Domain Controller ist ausgefallen, aber andere Domain Controller sind immer noch verfügbar. Siehe 'Wiederherstellung eines Domain Controllers (andere DC sind verfügbar) (S. 238)'.
- Alle Domain-Controller sind ausgefallen (oder es gab nur einen). Siehe 'Wiederherstellung eines Domain Controllers (keine anderen DC sind verfügbar) (S. 240)'.
- Die Active Directory-Datenbank ist beschädigt und der Active Directory-Dienst startet nicht. Siehe 'Wiederherstellung der Active Directory-Datenbank (S. 240).
- Bestimmte Informationen wurden versehentlich aus dem Active Directory gelöscht. Siehe 'Wiederherstellung versehentlich gelöschter Informationen (S. 241)'.

11.4.1 Wiederherstellung eines Domain-Controllers (andere DC sind verfügbar)

Wenn einer von mehreren Domain-Controllern (DCs) ausgefallen ist, ist der Active Directory-Dienst immer noch verfügbar. Daher werden andere Domain-Controller Daten enthalten, die neuer sind als die Daten im Backup.

In diesem Fall wird üblicherweise ein Typ von Wiederherstellung durchgeführt, der als *nicht autorisierte Wiederherstellung* bekannt ist. Nicht autorisierte Wiederherstellung bedeutet, dass die Wiederherstellung den aktuellen Status des Active Directorys nicht beeinflusst.

Auszuführende Schritte

Falls die Domain noch andere Domain-Controller hat, können Sie eine nicht autorisierte Wiederherstellung eines ausgefallenen Domain-Controllers auf eine der folgenden Arten durchführen:

- **Wiederherstellung eines Domain-Controllers** von einem Backup mithilfe eines bootfähigen Mediums. Stellen Sie sicher, dass es kein USN-Rollback-Problem (S. 242) gibt.

- **Neuerstellung eines Domain-Controllers**, indem Sie das Betriebssystem installieren und die Maschine zu einem neuen Domain-Controller machen (durch Verwendung des Tools `dcpromo.exe`).

Auf beide Aktionen folgt eine automatische *Replikation*. Die Replikation bringt die Domain-Controller-Datenbank auf den neuesten Stand. Stellen Sie einfach nur sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde. Sobald die Replikation abgeschlossen ist, ist der Domain-Controller aktuell und läuft wieder.

Wiederherstellung versus Neuerstellung

Neuerstellung erfordert nicht die Verfügbarkeit eines Backups. Eine Wiederherstellung ist normalerweise schneller als eine Neuerstellung. Eine Wiederherstellung ist jedoch in folgenden Fällen nicht möglich:

- Alle verfügbaren Backups sind älter als die 'Tombstone-Lebensdauer'. Tombstones werden während der Replikation verwendet, um sicherzustellen, dass ein auf einem Domain-Controller gelöschtest Objekt auch auf einem anderen Domain-Controller gelöscht wird. Eine korrekte Replikation ist daher nicht möglich, nachdem die Tombstones gelöscht wurden.
- Der Domain-Controller hatte eine Rolle für 'flexible einfache Mastervorgänge' (Flexible Single Master Operations, FSMO) inne – und Sie haben diese Rolle einem anderen Domain-Controller zugewiesen (Übernahme der Rolle). In diesem Fall würde eine Wiederherstellung des Domain-Controllers dazu führen, dass zwei Domain-Controller dieselbe FSMO-Rolle innerhalb der Domain innehaben und einen Konflikt verursachen.

Wiederherstellung eines Domain-Controllers, der eine FSMO-Rolle innehält.

Einige Domain-Controller halten eindeutige Rollen, die auch als 'flexible einfache Mastervorgänge'-Rollen (Flexible Single Master Operations roles, FSMO roles) oder Betriebsmaster-Funktionen (Operations Manager-Rollen) bekannt sind. Eine Beschreibung der FSMO-Rollen und ihres Umfangs (domänenweit oder gesamtstrukturweit) finden Sie im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/324801.

Vor Neuerstellung eines Domain-Controllers, der eine PDC-Emulator-Rolle innehielt, müssen Sie diese Rolle übernehmen. Anderenfalls werden Sie nicht in der Lage sein, den neuerstellten Domain-Controller der Domain hinzuzufügen. Sie können nach der Neuerstellung des Domain-Controllers diese Rolle rückübertragen. Weitere Information zum Übernehmen und Übertragen von FSMO-Rollen finden Sie im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/255504.

Um einzusehen, welche FSMO-Rollen welchem Domain-Controller zugewiesen sind, können Sie sich mit jedem aktuellen (live) Domain-Controller verbinden, indem Sie das Tool **`Ntdsutil`** verwenden, wie es im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/234790 beschrieben ist. Folgen Sie den Schritten, die im Abschnitt 'Verwenden des Programms NTDSUTIL' des Artikels beschrieben sind:

- Folgen Sie bei den Betriebssystemen Windows 2000 Server und Windows Server 2003 allen Schritten wie angegeben.
- Bei den Windows Server 2008-Betriebssystemen müssen Sie in dem Schritt, indem Sie aufgefordert werden, **Domänenverwaltung** einzugeben, stattdessen **Rollen** eingeben. Folgen Sie den anderen Schritten wie angegeben.

11.4.2 Wiederherstellung eines Domain-Controllers (keine anderen DC sind verfügbar)

Sollten alle Domain-Controller ausgefallen sein, dann wird die nicht autorisierte Wiederherstellung tatsächlich zu einer autorisierten: die aus dem Backup wiederhergestellten Objekte sind dann die neuesten, die verfügbar sind. Eine Replikation von Active Directory-Daten kann nicht stattfinden, weil es keine aktuellen (live) Domain-Controller gibt. Das bedeutet:

- Nach dem Backup durchgeführte Änderungen am Active Directory gehen verloren.
- Eine Neuerstellung des Domain-Controllers ist keine Option.
- Sogar ein Backup mit einer abgelaufenen Tombstone-Lebensdauer kann verwendet werden.

Sie müssen die Volumes wiederherstellen, in denen die Active Directory-Datenbankdateien (S. 226) gespeichert sind. Sollten in diesen Volumes weitere, wichtige Daten (außer dem Active Directory) gespeichert sein, dann kopieren Sie diese Daten vor der Wiederherstellung zu einem anderen Speicherort.

So stellen Sie einen Domain-Controller wieder her, wenn keine anderen Domain-Controller verfügbar sind

1. Stellen Sie sicher, dass das neueste Backup für die Wiederherstellung verwendet wird. Das ist wichtig, weil alle nach dem Backup am Active Directory durchgeführten Änderungen verlorengehen werden.
2. Stellen Sie den Domain-Controller von dem Backup wieder her, indem Sie ein bootfähiges Medium verwenden.
3. Starten Sie den Domain-Controller neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde.

11.4.3 Wiederherstellung der Active Directory-Datenbank

Sollten die Active Directory-Datenbankdateien beschädigt sein, der Domain-Controller aber noch im normalen Modus starten können, dann können Sie die Datenbank mit einer der folgenden Möglichkeiten wiederherstellen.

Höherstufen des Domain-Controllers

Bei dieser Art der Wiederherstellung ist die Datenbank nur dann verfügbar, falls die Domain noch andere Domain-Controller hat. Die Verfügbarkeit eines Backups ist nicht erforderlich.

Verwenden Sie zur Wiederherstellung der Datenbank das Tool **Dcpromo**, um den Domain-Controller mit der beschädigten Datenbank tieferzustufen – und dann, um diesen Domain-Controler anschließend wieder höherzustufen.

Fühlen Sie folgende Befehle aus, um den Domain-Controller erneut höherzustufen:

```
dcpromo /forceremoval

dcpromo /adv
```

Wiederherstellung der Datenbank von einem Backup

Bei dieser Art der Wiederherstellung kann die Datenbank unabhängig davon verwendet werden, ob die Domain noch weitere Domain-Controller hat.

Stellen Sie die Active Directory-Datenbankdateien (S. 226) wieder her, um die Datenbank wiederherzustellen. Falls Sie zusätzlich seit dem Backup irgendwelche Änderungen an den

Gruppenrichtlinienobjekten (GPOs) gemacht haben, müssen Sie außerdem den SYSVOL-Ordner (S. 232) wiederherstellen.

So stellen Sie die Active Directory-Datenbank von einem Backup aus wieder her

1. Starten Sie den Domain-Controller neu und drücken Sie während des Startvorgangs auf F8.
2. Wählen Sie im Fenster **Erweiterte Startoptionen** das Element **Verzeichnisdienst-Wiederherstellungsmodus**.
3. [Optional] Erstellen Sie eine Kopie der aktuellen Active Directory-Datenbankdatei, um die Änderungen bei Bedarf wieder rückgängig machen zu können.
4. Ändern Sie das ursprüngliche Konto des Acronis Agent Service auf das Administratorkonto des Verzeichnisdienst-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM).
   a. Öffnen Sie das Snap-in **Dienste**.
   b. Klicken Sie in der Liste der Dienste auf **Acronis Managed Machine Service**.
   c. Spezifizieren Sie in der Registerkarte **Anmelden**, bei **Dieses Konto**, den Benutzernamen und das Kennwort, welche Sie verwenden, um sich am Verzeichnisdienst-Wiederherstellungsmodus anzumelden – und klicken Sie dann auf **Aktivieren**.
   d. Klicken Sie in der Registerkarte **Allgemein** auf **Starten**. Klicken Sie nach dem Start des Dienstes auf **OK**.

   Details: Diese Änderung ist notwendig, weil der Acronis Agent Service auf einem Domain-Controller unter einem Domain-Benutzerkonto läuft, Domain-Benutzerkonten sind jedoch im Verzeichnisdienst-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM) nicht verfügbar.
5. Starten Sie Acronis Backup und stellen Sie die Datenbankdateien aus dem Backup wieder her. Stellen Sie bei Bedarf auch den SYSVOL-Ordner wieder her.

   Details: Weitere Informationen über die Pfade zu diesen Dateien und Ordnern finden Sie unter 'Active Directory-Backup (S. 232). Die Recovery-Prozedur ist ähnlich zu der, die im Abschnitt 'Wiederherstellung von Exchange-Server-Datenbankdateien (S. 236)' beschrieben ist.
6. Sollte die Domain andere Domain-Controller haben, dann stellen Sie sicher, dass kein USN-Rollback-Problem auftritt (S. 242).
7. Starten Sie den Domain-Controller im normalen Modus neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde.
8. Ändern Sie das Konto für den Acronis-Dienst wieder zurück auf das ursprüngliche, ähnlich wie in Schritt 4.

11.4.4 Wiederherstellung versehentlich gelöschter Informationen

Falls die Domain noch andere Domain-Controller hat, können Sie das Tool **`Ntdsutil`** verwenden, um eine autorisierte Wiederherstellung nur von bestimmten Einträgen durchführen zu können. Sie können beispielsweise ein unbeabsichtigt gelöschtes Benutzerkonto oder Computerkonto wiederherstellen.

So stellen Sie versehentlich gelöschte Informationen wieder her

1. Führen Sie die Schritte 1 - 5 der Anleitung zur 'Wiederherstellung der Active Directory-Datenbank (S. 240)' aus, um den Domain-Controller im Verzeichnisdienste-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM) neu zu starten und die Active Directory-Datenbank wiederherzustellen.
2. Führen Sie ohne vorhandenen DSRM folgenden Befehl aus:


```
Ntdsutil
```

3. Führen Sie in der Eingabeaufforderung des Tools folgende Befehle aus:

```
activate instance ntds
authoritative restore
```

4. Starten Sie in der Eingabeaufforderung des Tools den Befehl **`restore subtree`** oder **`restore object`** mit den benötigten Parametern.

   Folgender Befehl stellt beispielsweise das Benutzerkonto **`Manager`** in der Organisationseinheit **`Finance`** der Domain **`example.com`** wieder her:

```
restore object cn=Manager,ou=Finance,dc=example,dc=com
```

   Weitere Informationen über die Verwendung des Tools **`Ntdsutil`** finden Sie in dessen Dokumentation.

   Details: Andere Objekte werden von anderen Domain-Controllern repliziert, wenn Sie den Domain-Controller neu starten. Auf diese Weise stellen Sie die unbeabsichtigt gelöschten Objekte wieder her und behalten Sie die anderen Objekte auf dem neuesten Stand.

5. Starten Sie den Domain-Controller im normalen Modus neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde – und die wiederhergestellten Objekte verfügbar geworden sind.
6. Ändern Sie das Konto für den Acronis Agent Service wieder zurück auf das ursprüngliche Konto (wie in Schritt 4 des Abschnitts 'Wiederherstellung der Active Directory-Datenbank (S. 240)' beschrieben.

11.4.5 Vermeidung eines USN-Rollbacks

Sollte die Domain über zwei oder mehr Domain-Controller verfügen und sollten Sie einen der Controller oder seine Datenbank wiederherstellen müssen, dann sollten Sie Maßnahmen gegen eine Situation erwägen, die auch als 'USN-Rollback' bekannt ist.

Ein USN-Rollback ist unwahrscheinlich, wenn Sie einen kompletten Domain-Controller von einem VSS-basierten Laufwerk-Backup wiederherstellen.

Ein USN-Rollback ist dagegen deutlich wahrscheinlicher, wenn einer der folgenden Umstände zutrifft:

- Ein Domain-Controller wurde teilweise wiederhergestellt: es wurden nicht alle Laufwerke oder Volumes wiederhergestellt – oder nur die Active Directory-Datenbank.
- Ein Domain-Controller wurde von einem Backup wiederhergestellt, welches ohne VSS erstellt wurde. Das Backup wurde beispielsweise mit einem bootfähigen Medium erstellt. Oder die Option **VSS verwenden** (S. 109) war deaktiviert. Oder der VSS-Provider hatte eine Fehlfunktion.

Die folgenden Informationen helfen Ihnen, ein USN-Rollback mit einigen einfachen Schritten zu vermeiden.

Replikation und USNs

Ein Active Directory wird kontinuierlich zwischen den Domain-Controllern repliziert. Zu jedem Zeitpunkt kann es zu einem Active Directory-Objekt eine neuere Version auf einem Domain-Controller und eine ältere auf einem anderen geben. Um Konflikte und Informationsverluste zu vermeiden, verfolgt das Active Directory Objektversionen auf jedem Domain Controller und ersetzt veraltete Versionen mit aktuellen Versionen.

Um die Objektversionen zu verfolgen, verwendet das Active Directory Zahlen, die Update-Sequenznummern, USNs, Update Sequence Numbers oder Aktualisierungssequenznummern

genannt werden. Neuere Versionen von Active Directory-Objekten entsprechen höheren USNs. Jeder Domain Controller bewahrt die USNs von allen anderen Domain Controllern.

USN-Rollback

Nach Durchführung einer nicht autorisierten Wiederherstellung eines Domain Controllers oder seiner Datenbanken wird die aktuelle USN dieses Domain Controllers durch die alte (niedrigere) USN aus dem Backup ersetzt. Die anderen Domain-Controller wissen jedoch nichts von dieser Änderung. Sie haben immer noch die zuletzt bekannte (höhere) USN dieses Domain Controllers beibehalten.

Als Ergebnis treten folgende Probleme auf:

- Der wiederhergestellte Domain Controller verwendet ältere USNs für neue Objekte; er startet mit der alten USN aus dem Backup.
- Die anderen Domain Controller replizieren die neuen Objekte von dem wiederhergestellten Domain-Controller solange nicht, wie dessen USN niedriger bleibt als die USN, von der die anderen Domain-Controller wissen.
- Das Active Directory startet und hat verschiedene Objekte, die zu der gleichen USN korrespondieren, was bedeutet, dass Sie inkonsistent geworden ist. Diese Situation wird USN-Rollback genannt.

Sie müssen zur Vermeidung eines USN-Rollbacks den Domain-Controller über die Tatsache informieren, dass er wiederhergestellt wurde.

So vermeiden Sie ein USN-Rollback

1. Booten Sie direkt nach der Wiederherstellung eines Domain-Controllers oder seiner Datenbanken den wiederhergestellten Domain-Controller und drücken Sie während des Startvorgangs auf F8.
2. Wählen Sie im Fenster **Erweiterte Startoptionen** den Eintrag **Verzeichnisdienst-Wiederherstellungsmodus** – und melden Sie sich dann am Verzeichnisdienste-Wiederherstellungsmodus (DSRM) an.
3. Öffnen Sie den Registry-Editor und erweitern Sie den folgenden Registry-Schlüssel:
   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
   ```
4. Überprüfen Sie in diesem Registry-Schlüssel den Wert **DSA Previous Restore Count**. Sollte der Wert vorhanden sein, dann notieren Sie sich seine Einstellung. Fügen Sie den Wert nicht hinzu, falls er fehlen sollte.
5. Fügen Sie diesem Registry-Schlüssel folgenden Wert hinzu:
   - Werttyp: **DWORD-Wert (32-Bit)**
   - Wertname: **Von Sicherung wiederhergestellte Datenbank**
   - Datenwert: **1**
6. Starten Sie den Domain-Controller im normalen Modus neu.
7. [Optional] Öffnen Sie nach dem Neustart des Domain Controllers die Ereignisanzeige, erweitern Sie **Anwendungs- und Dienstprotokolle** und wählen Sie das Protokoll **Verzeichnisdienste**. Schauen Sie im Protokoll **Verzeichnisdienste** nach einem kürzlichen Eintrag mit der Ereignis-ID 1109. Sollten Sie diesen Eintrag finden, dann klicken Sie doppelt darauf, um sicherzustellen, dass das Attribut **InvocationID** geändert wurde. Das bedeutet, dass die Active Directory-Datenbank aktualisiert wurde.
8. Öffnen Sie den Registry-Editor und überprüfen Sie, dass die Einstellung im Wert **DSA Previous Restore Count** im Vergleich zu Schritt 4 um den Wert 1 gestiegen ist. Sollte der Wert **DSA Previous Restore Count** in Schritt 4 gefehlt haben, dann überprüfen Sie, dass er nun vorhanden ist und seine Einstellung **1** beträgt.

Sollten Sie eine andere Einstellung sehen (und den Eintrag für die Ereignis-ID 1109 nicht finden können), dann stellen Sie sicher, dass der wiederhergestellte Domain-Controller über die aktuellen Service Packs verfügt und wiederholen Sie dann die komplette Prozedur.

Weitere Details über USNs und USN-Rollback finden Sie in folgendem Microsoft Technet-Artikel: http://technet.microsoft.com/de-de/library/virtual_active_directory_domain_controller_virtualization_hyperv.aspx.

11.5 Wiederherstellung von SharePoint-Daten

Verschiedene SharePoint-Server und SharePoint-Datenbanken werden auf unterschiedliche Art wiederhergestellt.

- Um einzelne Laufwerke oder Volumes eines Front-End-Webservers wiederherzustellen, können Sie entweder mit der grafischen Benutzeroberfläche von Acronis Backup einen Recovery-Task erstellen (S. 112) – oder den Server mit einem bootfähigen Medium (S. 189) starten und dort die Wiederherstellung konfigurieren.

  Auf gleiche Art können Sie einen SQL Server wiederherstellen.
- Inhaltsdatenbanken können mithilfe des Agenten für SQL oder des Agenten für Windows wiederhergestellt werden. Weitere Details finden Sie unter 'Wiederherstellung einer Inhaltsdatenbank (S. 244)'.
- Konfigurations- und Dienstdatenbanken werden als Dateien wiederhergestellt. Weitere Details finden Sie unter 'Wiederherstellung von Konfigurations- und Dienstdatenbanken (S. 246)'.
- Sie können auch einzelne SharePoint-Elemente wiederherstellen (wie Websites, Listen, Dokumentbibliotheken und anderes). Weitere Details finden Sie unter 'Wiederherstellung einzelner Elemente (S. 247)'.

11.5.1 Wiederherstellung einer Inhaltsdatenbank

Dieses Thema beschreibt die Wiederherstellung einer Inhaltsdatenbank zu einer ursprünglichen SharePoint-Farm unter Verwendung von Acronis Backup.

Die Wiederherstellung zu einer 'nicht ursprünglichen' Farm ist eine kompliziertere Prozedur. Diese Schritte variieren in Abhängigkeit von der Farm-Konfiguration und anderen Parametern der Produktionsumgebung.

Eine Inhaltsdatenbank mit dem Agenten für SQL wiederherstellen

Diese Methode ermöglicht es Ihnen, eine Datenbank aus dem Single-Pass-Backup einer Maschine wiederherzustellen, auf der der SQL Server läuft.

So stellen Sie eine Inhaltsdatenbank wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Datenbank wiederherstellen wollen. Der Agent für SQL muss auf dieser Maschine installiert sein.
2. Stellen Sie die Datenbank gemäß der Beschreibung im Abschnitt 'SQL-Datenbanken zu Instanzen wiederherstellen' zu einer Instanz wieder her.
3. Falls Sie die Datenbank nicht zu dem ursprünglichen SQL Server der ursprünglichen SharePoint-Farm wiederhergestellt haben, dann fügen Sie die wiederhergestellte Datenbank an die Farm an. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
   -WebApplication <Site-URL>
   ```


Bei SharePoint 2007:

```
stsadm.exe -o addcontentdb -url <Site-URL> -databasename <Datenbank>
-databaseserver <Datenbankserver>
```

Eine Inhaltsdatenbank mit dem Agenten für Windows wiederherstellen

Diese Methode ermöglicht es Ihnen, eine Datenbank aus dem Laufwerk-Backup einer Maschine wiederherzustellen, auf der der SQL Server läuft.

So stellen Sie eine Inhaltsdatenbank zu dem ursprünglichen SQL Server wieder her

1. Falls der Dienst 'Windows SharePoint Services Timer' läuft, stoppen Sie den Dienst und warten Sie einige Minuten, damit irgendwelche laufenden gespeicherten Prozeduren abgeschlossen werden können. Starten Sie den Dienst nicht neu, bis Sie alle Datenbanken, die wiederhergestellt werden müssen, auch wiederhergestellt haben.
2. Falls Sie die Datenbank zu dem ursprünglichen Speicherplatz auf dem Laufwerk wiederherstellen, dann tun Sie Folgendes:
   a. Bringen Sie die Zieldatenbank offline.
   b. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 234)' beschrieben wieder her, mit Ausnahme des Schritts zum Anfügen der Datenbank (die Datenbank ist bereits angefügt).
   c. Bringen Sie die wiederhergestellte Datenbank online.

   Falls Sie die Datenbank zu einem anderen Speicherort auf dem Laufwerk wiederherstellen, dann stellen Sie die Datenbankdateien wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 234)' beschrieben wieder her, einschließlich des Schrittes zum Anfügen der Datenbank.
3. Starten Sie den Windows SharePoint Services Timer-Dienst.

So stellen Sie eine Inhaltsdatenbank zu einem anderen SQL auf der ursprünglichen Farm wieder her

1. Entfernen Sie von der SharePoint-Farm diejenige Datenbank, die Sie später wiederherstellen werden. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Dismount-SPContentDatabase <Datenbank>
   ```

   Falls Sie mehrere Inhaltsdatenbanken mit demselben Namen haben, müssen Sie statt des Namens die GUID der Inhaltsdatenbank in diesem Befehl verwenden. Um die GUID der Inhaltsdatenbank abfragen zu können, müssen Sie die das Cmdlet ***`Get-SPContentDatabase`*** *ohne Argumente ausführen.*

   Bei SharePoint 2007:

   ```
   stsadm -url <Webapplikations-URL> –o deletecontentdb –databasename <Datenbank>
   ```
2. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 234)' beschrieben wieder her, einschließlich des Schrittes zum Anfügen der Datenbank.
3. Fügen Sie die wiederhergestellte Datenbank an die SharePoint-Farm an. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
   -WebApplication <Site-URL>
   ```

   Bei SharePoint 2007:

   ```
   stsadm.exe -o addcontentdb -url <Site-URL> -databasename <Datenbank>
   -databaseserver <Datenbankserver>
   ```


11.5.2 Wiederherstellung von Konfigurations- und Dienstdatenbanken

Konfigurations- und Dienstdatenbanken müssen mit anderen Datenbanken synchronisiert werden. Es ist daher empfehlenswert, Konfigurations- und Dienstdatenbanken entweder zusammen mit Inhaltsdatenbanken wiederherzustellen – oder zu ihrem letzten Zeitpunkt (falls die Inhaltsdatenbanken keine Wiederherstellung benötigen).

Die Konfigurationsdatenbank enthält Host-Namen der Farm-Server. Daher können Sie die Konfigurationsdatenbank nur zu der ursprünglichen SharePoint-Farm wiederherstellen. Dienstdatenbanken können zu einer nicht ursprünglichen Farm wiederhergestellt werden.

So stellen Sie die Konfigurationsdatenbank wieder her

1. Stoppen Sie auf dem Server, der die Website **Zentraladministration** ausführt, im Snap-in **Dienste** die in der unteren Tabelle aufgelisteten Dienste.
2. Führen Sie folgenden Befehl auf dem Server aus, der die Site **Zentraladministration** ausführt:
   ```
   iisreset /stop
   ```
3. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 234)' beschrieben wieder her.
4. Starten Sie die SharePoint-Dienste wieder, die zuvor gestoppt wurden.

SharePoint 2007-Dienste	SharePoint 2010-Dienste	SharePoint 2013-Dienste
▪ **Microsoft Dienst für einmaliges Anmelden** ▪ **Office-Startprogrammdienst für die Dokumentkonvertierung** ▪ **Office-Lastenausgleichsmodul-Dienst für die Dokumentkonvertierung** ▪ **Office SharePoint Server-Suchdienst** ▪ **Windows SharePoint Services-Verwaltung** ▪ **Windows SharePoint Services-Suche** ▪ **Windows SharePoint Services-Timer** ▪ **Windows SharePoint Services-Ablaufverfolgung** ▪ **Windows SharePoint Services VSS Writer**	▪ **SharePoint 2010-Verwaltungsdienst** ▪ **SharePoint 2010 Timerdienst** ▪ **SharePoint 2010-Ablaufverfolgungsdienst** ▪ **SharePoint 2010 User Code Host** ▪ **SharePoint 2010 VSS Writer** ▪ **WWW-Publishingdienst** ▪ **SharePoint Server Search 14** ▪ **SharePoint Foundation Search V4** ▪ **Web Analytics-Datenverarbeitungsdienst** ▪ **Web Analytics-Webdienst**	▪ **SharePoint-Administration** ▪ **SharePoint-Timer** ▪ **SharePoint-Ablaufverfolgung** ▪ **SharePoint User Code Host** ▪ **SharePoint VSS Writer** ▪ **WWW-Publishingdienst** ▪ **SharePoint Server-Suche**

So stellen Sie eine Dienstdatenbank wieder her

1. Stoppen Sie die Dienste, die mit den wiederherzustellenden Datenbanken assoziiert sind. Gehen Sie folgendermaßen vor:
   a. Öffnen Sie die Seite **Zentraladministration**.
   b. Wählen Sie eine der nachfolgenden Varianten:

Wählen Sie in SharePoint 2010 (oder höher) **Systemeinstellungen** –> **Dienste auf dem Server verwalten**.

Wählen Sie in SharePoint 2007 **Vorgänge** –> **Dienste auf dem Server**.

c. Klicken Sie zum Ändern des Servers, auf dem Sie den Dienst stoppen wollen, in der Liste **Server** auf **Server ändern** und klicken Sie dann auf den gewünschten Server-Namen.
d. Standardmäßig werden nur konfigurierbare Dienste angezeigt. Klicken Sie in der Liste **Ansicht** auf **Alle**, um alle Dienste anzuzeigen.
e. Klicken Sie auf **Beenden** in der Spalte **Aktion** des entsprechenden Dienstes, um einen Dienst zu stoppen.
f. Klicken Sie auf **OK**, um den Dienst zu stoppen.

2. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 234)' beschrieben wieder her.
3. Starten Sie, ähnlich wie in Schritt 1, die mit den Datenbanken assoziierten Dienste.

11.5.3 Wiederherstellung einzelner Elemente

Verwenden Sie eine der folgenden dreit Methoden zur Wiederherstellung einzelner SharePoint-Elemente:

- Acronis SharePoint Explorer verwenden. Dieses Tool ermöglicht es Ihnen, SharePoint-Elemente von Single-Pass-Laufwerk- und Anwendungs-Backups, von einer angebundenen Datenbank oder von Datenbankdateien wiederherzustellen.

  Um das Tool verwenden zu können, müssen Sie eine funktionierende SharePoint-Farm haben. Sie müssen außerdem eine Acronis Backup-Lizenz erwerben, die SharePoint-Backups unterstützt.

  Sie können auf Acronis SharePoint Explorer zugreifen, indem Sie im Menü **Extras** der Acronis Backup Management Console auf den Befehl **SharePoint-Daten extrahieren** klicken. Weitere Informationen über das Tool finden Sie in dessen Dokumentation: http://www.acronis.de/support/documentation/ASPE/.
- Anfügen der Inhaltsdatenbank an eine 'nicht ursprüngliche' SharePoint-Farm (beispielsweise eine SharePoint-Wiederherstellungsfarm).

  Es ist notwendig, die Inhaltsdatenbank an eine nicht ursprüngliche SharePoint-Farm anzufügen, weil jedes Objekt in einer Farm eine eindeutige ID haben muss. Sie können daher die Datenbank nicht an die ursprüngliche Farm anfügen.
- Wiederherstellung von einer nicht angefügten Datenbank Diese Methode ist für SharePoint 2007 nicht verfügbar.

  Diese Methode ermöglicht es Ihnen nur, die folgenden Elementtypen wiederherzustellen: Websites, Listen oder Dokumentbibliotheken.

So stellen Sie SharePoint-Elemente durch Anfügen der Inhaltsdatenbank zu einer Farm wieder her

1. Fügen Sie die Inhaltsdatenbank einer SQL Server-Instanz an, wie es in den Schritten 1-5 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 235)' beschrieben ist.
2. Fügen Sie die Inhaltsdatenbank einer nicht ursprünglichen SharePoint-Farm an. Gehen Sie folgendermaßen vor:
   a. Stellen Sie sicher, dass Sie diese Prozedur unter einem Farm-Administratorkonto durchführen, welches ein Mitglied der Rolle **db_owner** der Datenbank ist. Ist das nicht der Fall, dann verwenden Sie Microsoft SQL Server Management Studio, um das Konto dieser Rolle hinzuzufügen.

b. Führen Sie folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
   -WebApplication <Website-URL>
   ```

   Bei SharePoint 2007:

   ```
   stsadm.exe -o addcontentdb -url <Website-URL> -databasename <Datenbank>
   -databaseserver <Datenbankserver>
   ```

3. Öffnen Sie die SharePoint-Website und wählen Sie das herunterzuladende Dokument.
4. Trennen Sie die Inhaltsdatenbank nach dem Abschluss des Downloads wieder von der SharePoint-Farm.
5. Trennen Sie die Datenbank und dann das zuvor gemountete Volume, wie in den Schritten 7-8 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 235)' beschrieben.

So stellen Sie SharePoint-Elemente von einer nicht angefügten Datenbank wieder her

1. Fügen Sie die Inhaltsdatenbank einer SQL Server-Instanz an, wie es in den Schritten 1-5 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 235)' beschrieben ist.
2. Stellen Sie die Daten gemäß der Beschreibung unter 'http://technet.microsoft.com/de-de/library/hh269602' wieder her.
3. Trennen Sie die Datenbank und dann das zuvor gemountete Volume, wie in den Schritten 7-8 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 235)' beschrieben.

12 Eine verwaltete Maschine administrieren

In diesem Abschnitt werden die Ansichten beschrieben, die über den Verzeichnisbaum 'Navigation' einer mit der Konsole verbundenen verwalteten Maschine verfügbar sind und erklärt, wie Sie mit diesen Ansichten arbeiten. In diesem Abschnitt werden außerdem zusätzliche Aktionen behandelt, die auf einer verwalteten Maschine ausgeführt werden können – wie das Wechseln einer Lizenz, das Einstellen der **Maschinen-Optionen** oder das Einsammeln von Systeminformationen.

12.1 Backup-Pläne und Tasks

Die Ansicht **Backup-Pläne und Tasks** informiert Sie über die Datensicherung auf einer bestimmten Maschine. Sie ermöglicht Ihnen, Backup-Pläne und Tasks zu überwachen und zu verwalten.

Sehen Sie unter Backup-Plan-Ausführungsstadium (S. 251) nach, um herauszufinden, was ein Backup-Plan auf einer Maschine gerade tut. Das Ausführungsstadium eines Backup-Plans entspricht dem kumulativen Stadium all seiner jüngsten Aktivitäten. Der Status eines Backup-Plans (S. 252) hilft Ihnen bei der Einschätzung, ob die Daten erfolgreich gesichert wurden.

Um den aktuellen Fortschritt eines Tasks im Überblick zu behalten, verfolgen Sie sein Stadium (S. 253). Prüfen Sie den Status (S. 253) eines Tasks, um sein Ergebnis in Erfahrung zu bringen.

Typischer Arbeitsablauf

- Nutzen Sie Filter, um in der Backup-Plan-Tabelle die gewünschten Backup-Pläne (Tasks) zu sehen. Standardmäßig zeigt die Tabelle die Pläne der verwalteten Maschine nach Namen sortiert an. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 18)'.
- Wählen Sie in der Backup-Tabelle den Backup-Plan (Task).
- Verwenden Sie die Schaltflächen der Symbolleiste, um eine Aktion auf den gewählten Plan (Task) anzuwenden. Zu Details siehe 'Aktionen für Backup-Pläne und Tasks (S. 249)'.
- Verwenden Sie den Bereich 'Informationen' im unteren Teil des Fensters, um detaillierte Informationen über den gewählten Plan (Task) einsehen zu können. Die Leiste ist standardmäßig eingeklappt. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol klicken. Der Inhalt der Leiste wird außerdem auch in den Fenstern **Plan-Details** (S. 258) und **Task-Details** (S. 260) angezeigt.

12.1.1 Aktionen für Backup-Pläne und Tasks

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen für Backup-Pläne und Tasks.

Einschränkungen

- Ohne administrative Berechtigungen kann ein Benutzer auf einer Maschine keine zu anderen Benutzern gehörenden Pläne oder Tasks ausführen oder modifizieren.
- Es ist nicht möglich, einen aktuell laufenden Backup-Plan oder Task zu modifizieren oder zu löschen.

Aufgabe	**Lösung**
Einen neuen Backup-Plan oder Task erstellen	Klicken Sie auf **Neu** und wählen Sie eine der folgenden Optionen: ▪ Backup-Plan (S. 38)

<table>
<tr><th>Aufgabe</th><th>Lösung</th></tr>
<tr><td></td><td>▪ Recovery-Task (S. 112)
▪ Validierungstask (S. 172)</td></tr>
<tr><td>Details eines Plans/Tasks einsehen</td><td>Klicken Sie auf Details.
Überprüfen Sie im Fenster Plan-Details (S. 258) oder Task-Details (S. 260) die entsprechenden Angaben.</td></tr>
<tr><td>Log eines Plans/Tasks einsehen</td><td>Klicken Sie auf Log.
Sie gelangen dadurch in die Ansicht Log (S. 260), die eine Liste von Log-Einträgen enthält, die in Bezug auf die Plan-/Task-Aktivitäten gruppiert sind.</td></tr>
<tr><td>Einen Plan/Task ausführen</td><td><u>Backup-Plan</u>
1. Klicken Sie auf Ausführen.
2. Wählen Sie aus dem Listenfeld den Task des Plans aus, den Sie ausführen müssen.
Die Ausführung des Backup-Plans startet auch unmittelbar den dazugehörigen, ausgewählten Task, ungeachtet seiner Planung und anderer Konditionen.
<u>Task</u>
Klicken Sie auf Ausführen.
Die Ausführung des Tasks startet unmittelbar, ungeachtet seiner Planung und anderer Bedingungen.</td></tr>
<tr><td>Einen Plan/Task stoppen</td><td>Klicken Sie auf Stopp.
<u>Backup-Plan</u>
Einen laufenden Backup-Plan zu stoppen bedeutet auch, alle seine Tasks zu stoppen. Folglich werden alle Task-Aktionen abgebrochen.
<u>Task</u>
Das Stoppen eines Tasks führt zum Abbruch seiner jeweiligen Aktion (Recovery, Validierung, Export, Konvertierung etc.). Der Task wechselt in das Stadium Inaktiv. Die Task-Planung bleibt aber, sofern erstellt, weiter gültig. Um die Aktion abzuschließen, müssen Sie den Task erneut ausführen.
Was passiert, wenn Sie einen Recovery-Task stoppen?
▪ Wiederherstellung von Laufwerken: Die abgebrochene Aktion kann zu Veränderungen auf dem Ziellaufwerk führen. In Abhängig von der seit Task-Ausführung verstrichenen Zeit ist das Ziellaufwerk möglicherweise nicht initialisiert, der Speicherplatz nicht zugeordnet oder wurden einige Volumes wiederhergestellt, andere jedoch nicht. Führen Sie den Task erneut aus, um das komplette Laufwerk wiederherzustellen.
▪ Wiederherstellung von Volumes: Das Ziel-Volume wird gelöscht und der entsprechende Speicherplatz wird 'nicht zugeordnet' – das gleiche Ergebnis, wie beim Fehlschlagen einer Wiederherstellung. Führen Sie den Task erneut aus, um das verlorene Volume wiederherzustellen.
▪ Wiederherstellung von Dateien und Ordnern: Die abgebrochene Aktion kann zu Veränderungen im Zielordner führen. In Abhängig von der seit Task-Ausführung verstrichenen Zeit wurden einige Dateien möglicherweise wiederhergestellt, andere wiederum nicht. Führen Sie den Task erneut aus, um alle Dateien wiederherzustellen.</td></tr>
</table>

Aufgabe	Lösung
Einen Plan/Task editieren	Klicken Sie auf **Bearbeiten**. Die Bearbeitung eines Backup-Plans wird auf dieselbe Art durchgeführt wie das Erstellen (S. 38), mit Ausnahme folgender **Einschränkungen**: Beim Bearbeiten eines Backup-Plans ist es nicht immer möglich, alle Optionen für Backup-Schemata zu verwenden, falls das erstellte Archiv nicht leer ist (d.h. Backups enthält). 1. Es ist nicht möglich, das Schema zu 'Großvater-Vater-Sohn' oder 'Türme von Hanoi' zu ändern. 2. Sie können die Zahl der Level nicht ändern, falls das Schema 'Türme von Hanoi' verwendet wird. In allen anderen Fällen kann das Schema verändert werden und sollte so weiterarbeiten, als wären bereits existierende Archive durch ein neues Schema erstellt worden. Bei leeren Archiven sind alle Veränderungen möglich.
Einen Backup-Plan klonen	Klicken Sie auf **Klonen**. Der Klon des ursprünglichen Backup-Plans wird mit dem Standardnamen '*Klon von <ursprünglicher Plan-Name>*' erstellt. Der geklonte Plan wird unmittelbar nach dem Klonvorgang deaktiviert, damit er nicht gleichzeitig mit dem ursprünglichen Plan ausgeführt wird. Sie können die Einstellungen des geklonten Plans bearbeiten, bevor Sie ihn dann aktivieren.
Einen Plan aktivieren	Klicken Sie auf **Aktivieren**. Der zuvor deaktivierte Backup-Plan wird wieder neu gemäß seiner Planung ausgeführt.
Einen Plan deaktivieren	Klicken Sie auf **Deaktivieren**. Der Backup-Plan wird nicht mehr gemäß seiner Planung ausgeführt. Er kann jedoch manuell gestartet werden. Der Plan verbleibt ansonsten auch nach einer manuellen Ausführung deaktiviert. Der Plan wird wieder wie normal ausgeführt, wenn Sie ihn erneut aktivieren.
Einen Plan exportieren	Klicken Sie auf **Exportieren**. Spezifizieren Sie Pfad und Namen für die resultierende Datei. Zu weiteren Informationen siehe 'Export und Import von Backup-Plänen (S. 254)'.
Einen Plan importieren	Klicken Sie auf **Importieren**. Spezifizieren Sie den Pfad und Namen der Datei, die einen zuvor exportierten Plan enthält. Zu weiteren Informationen siehe 'Export und Import von Backup-Plänen (S. 254)'.
Einen Plan/Task löschen	Klicken Sie auf **Löschen**.

12.1.2 Stadien und Statuszustände von Backup-Plänen und Tasks

12.1.2.1 Ausführungsstadien von Backup-Plänen

Das Stadium eines Backup-Plans entspricht dem kumulativen Stadium aller Tasks/Aktivitäten dieses Plans.

	Stadium	Wie es bestimmt wird	Handhabung
1	**Benutzereingriff erforderlich**	Wenigstens ein Task erfordert einen Benutzereingriff. Siehe anderenfalls Punkt 2.	Identifizieren Sie die Tasks, die eine Interaktion erfordern (das Programm zeigt an, was zu tun ist) –> Stoppen Sie die betreffenden Tasks oder ermöglichen Sie ihre Ausführung (wechseln Sie das Medium, sorgen Sie für zusätzlichen Platz im Depot, ignorieren Sie Lesefehler, erstellen Sie eine fehlende Acronis Secure Zone).
2	**Läuft**	Wenigstens ein Task wird ausgeführt. Siehe anderenfalls Punkt 3.	Es ist keine Handlung nötig.
3	**Wartend**	Wenigstens ein Task befindet sich in Wartestellung. Siehe anderenfalls Punkt 4.	Warten auf Bedingung. Diese Situation ist recht gängig, jedoch kann eine zu lange Backup-Verzögerung riskant sein. Die Lösung kann das Einstellen der maximalen Verzögerung (S. 108) sein, nach der der Task auf jeden Fall startet – oder dass Sie die entsprechende Bedingung erzwingen (beispielsweise dem betreffenden Benutzer zur Abmeldung auffordern oder eine benötigte Netzwerk-Verbindung einschalten). Wartend, während ein anderer Task die benötigten Ressourcen sperrt. Eine einmalige Wartesituation kann entstehen, wenn ein Task-Start verzögert wird oder eine Task-Ausführung aus bestimmten Gründen wesentlich länger als gewöhnlich dauert und daher einen anderen Task an der Ausführung hindert. Diese Situation wird automatisch gelöst, wenn der blockierende Task seinen Abschluss findet. Erwägen Sie, einen zu lange festhängenden Task zu stoppen, um dem nachfolgenden den Start zu ermöglichen. Eine andauernde Überlappung von Tasks kann das Ergebnis inkorrekt angelegter Zeit- bzw. Backup-Pläne sein. In solchen Fällen macht es natürlich Sinn, den entsprechenden Plan zu editieren.
4	**Untätig**	Alle Tasks befinden sich in Ruhestellung.	Es ist keine Handlung nötig.

12.1.2.2 Backup-Plan-Statuszustände

Ein Backup-Plan kann einen von folgenden Statuszuständen haben: **Fehler, Warnung, OK**.

Der Status eines Backup-Plans ergibt sich aus den Ergebnissen, die die Tasks/Aktivitäten dieses Plans bei ihren letzten Ausführungen gemeldet haben.

	Status	Wie es bestimmt wird	Handhabung
1	**Fehler**	Wenigstens ein Task ist fehlgeschlagen. Siehe anderenfalls Punkt 2.	Identifizieren Sie die fehlgeschlagenen Tasks –> Überprüfen Sie die Task-Ereignismeldungen im Log, um die Fehlerursache zu ermitteln und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie die Fehlerursache –> [optional] Starten Sie den fehlgeschlagenen Task manuell ▪ Bearbeiten Sie den lokalen Plan, falls der Fehler bei ihm lag, um sein zukünftiges Versagen zu verhindern.

2	**Warnung**	Wenigstens ein Task wurde mit Warnungen abgeschlossen. Siehe anderenfalls Punkt 3.	Prüfen Sie das Log, um die Warnungen zu lesen –> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.
3	**OK**	Alle Tasks wurden erfolgreich abgeschlossen.	Es ist keine Handlung nötig. Beachten Sie, dass ein Backup-Plan 'OK' sein kann, wenn bisher keiner der Tasks gestartet wurde.

12.1.2.3 Task-Stadien

Ein Backup-Task kann sich in einem der folgenden Stadien befinden: **Untätig**; **Wartend**; **Läuft**; **Benutzereingriff erforderlich**. Das anfängliche Task-Stadium ist **Untätig**.

Sobald der Task manuell gestartet wurde oder das als Auslöser spezifizierte Ereignis eingetreten ist, wechselt der Task entweder in das Stadium **Läuft** oder **Wartend**.

Läuft

Ein Task wechselt in das Stadium **Läuft**, wenn das im Scheduler definierte Ereignis eintritt UND alle im Backup-Plan definierten Bedingungen zutreffen UND kein anderer Task läuft, der benötigte Ressourcen blockiert. In diesem Fall verhindert also nichts die Ausführung des Tasks.

Wartend

Ein Task wechselt in das Stadium **Wartend**, wenn er im Begriff ist zu starten und dabei jedoch bereits ein anderer, die gleichen Ressourcen benutzender Task ausgeführt wird. Das bedeutet, dass auf einer Maschine nicht mehr als ein Backup-Task gleichzeitig laufen kann. Genauso wenig ist es möglich, dass ein Backup- und ein Recovery-Task gleichzeitig laufen können, falls sie dieselbe Ressource verwenden. Sobald der andere Task die Ressource freigibt, wechselt der wartende Task in das Stadium **Läuft**.

Ein Task kann außerdem in das Stadium **Wartend** wechseln, wenn das im Scheduler spezifizierte Ereignis zwar erfolgt, jedoch die im Backup-Plan definierten Bedingungen nicht erfüllt sind. Zu Details siehe 'Task-Startbedingungen (S. 108)'.

Benutzereingriff erforderlich

Jeder laufende Task kann sich selbst in das Stadium **Benutzereingriff erforderlich** versetzen, falls eine Benutzerinteraktion nötig ist, wie etwa ein Medienwechsel oder das Ignorieren eines Lesefehlers. Das nächste Stadium kann **Untätig** sein (falls der Benutzer wählt, dass der Task gestoppt wird) oder **Läuft** (bei Wahl von 'Ignorieren/Wiederholen' oder einer anderen Handlung, etwa einem Neustart, die den Task in das Stadium **Läuft** versetzen kann).

12.1.2.4 Task-Statuszustände

Ein Task kann sich in einem von folgenden Statuszuständen befinden: **Fehler**; **Warnung**; **OK**.

Der Status eines Tasks wird aus dem Ergebnis der letzten Ausführung des Tasks ermittelt.

	Status	Wie es bestimmt wird	Handhabung
1	**Fehler**	Das letzte Ergebnis ist „Fehlgeschlagen“	Identifizieren Sie den fehlgeschlagenen Task –> Überprüfen Sie das Task-Log, um die Fehlerursache zu ermitteln, und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie die Fehlerursache –> [optional] Starten Sie den fehlgeschlagenen Task manuell

			▪ Bearbeiten Sie den fehlgeschlagenen Task, um zukünftiges Misslingen zu verhindern
2	**Warnung**	Das letzte Ergebnis ist „Mit Warnung abgeschlossen“ oder der Task wurde gestoppt.	Prüfen Sie das Log, um die Warnungen zu lesen –> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.
3	**OK**	Das letzte Ergebnis ist „Erfolgreich abgeschlossen“ oder „Noch nicht ausgeführt“	Das Stadium 'Noch nicht ausgeführt' bedeutet, dass der Task noch nie gestartet wurde, oder dass er bereits gestartet, jedoch noch nicht abgeschlossen wurde und daher sein Ergebnis noch nicht verfügbar ist. Sie können auf Wunsch herausfinden, warum der Task bisher noch nicht gestartet wurde.

12.1.3 Backup-Pläne exportieren und importieren

Die Export-Aktion erstellt eine Datei mit der kompletten Konfiguration des Backup-Plans. Sie können die Datei importieren, um so den exportierten Backup-Plan auf einer anderen Maschine erneut nutzen zu können.

Sie können die Pläne in der grafischen Benutzeroberfläche von Acronis Backup beim Importieren bearbeiten (oder auch später). Backup-Pläne werden in .xml-Dateien exportiert, so dass Sie die exportierten Dateien der Backup-Pläne (S. 255) auch mit einem Text-Editor bearbeiten können. Kennwörter werden in den exportierten Dateien verschlüsselt.

Anwendungsbeispiele

- **Neuinstallation des Agenten**

  Exportieren Sie die Backup-Pläne, bevor Sie den Agenten neu installieren – nach der Neuinstallation können Sie diese dann wieder importieren.

- **Deployment eines Backup-Plans auf multiple Maschinen**

  Sie wollen denselben Backup-Plan auf mehreren Maschinen verwenden. Exportieren Sie den Plan von einer der Maschinen und verteilen Sie ihn als Datei (S. 257) auf die anderen Maschinen.

Anmeldedaten anpassen

Bevor Sie einen Backup-Plan exportieren, der später in einer anderen Maschine importiert wird, sollten Sie das Benutzerkonto überprüfen, unter dem der Plan läuft (**Bearbeiten** –> **Plan-Parameter** –> **Anmeldedaten des Tasks, Kommentare, Bezeichnung anzeigen** –> **Anmeldedaten des Plans**).

Der Plan wird auf einer anderen Maschine erfolgreich ausgeführt, falls der Wert für die **Anmeldedaten des Plans** entweder **Anmeldedaten des Acronis Service** lautet oder **Ausführen als: ... (Aktueller Benutzer)**. Falls der Parameter **Anmeldedaten des Plans** ein bestimmtes Benutzerkonto enthält, wird der Plan nur starten, wenn auf der betreffenden Maschine ein identisches Konto vorhanden ist. Sie müssen daher möglicherweise eine der folgenden Aktionen ausführen:

- Erstellen Sie ein Konto mit identischen Anmeldedaten auf der Maschine, auf der der Plan importiert wird.
- Bearbeiten Sie die Anmeldedaten in der exportierten Datei, bevor Sie diese importieren. Zu Details siehe die Exportdatei bearbeiten (S. 255).
- Bearbeiten Sie die Anmeldedaten nach Importieren des Plans.

Auszuführende Schritte

So exportieren Sie einen Backup-Plan

1. Wählen Sie einen Backup-Plan in der Ansicht **Backup-Pläne und Tasks**.
2. Klicken Sie auf **Exportieren**.
3. Spezifizieren Sie Pfad und Namen für die Exportdatei.
4. Bestätigen Sie Ihre Wahl.

So importieren Sie einen Backup-Plan

1. Klicken Sie in der Ansicht **Backup-Pläne und Tasks** auf **Importieren**.
2. Spezifizieren Sie Pfad und Namen für die Exportdatei.
3. Bestätigen Sie Ihre Wahl.
4. Falls Sie den neu importierten Backup-Plan bearbeiten müssen, dann wählen Sie ihn in der Ansicht **Backup-Pläne und Tasks** aus und klicken Sie dann auf **Bearbeiten**. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie dann auf **Speichern**.

12.1.3.1 Die Exportdatei bearbeiten

Die Exportdatei ist eine .xml-Datei und kann daher mit einem Texteditor bearbeitet werden.

Und so können Sie einige nützliche Änderungen vornehmen.

So modifizieren Sie Anmeldedaten

In der Export-Datei enthalten die Tags **<login>** den Benutzernamen und die Tags **<password>** das Benutzerkennwort.

Ändern Sie zum Modifizieren der Anmeldedaten die Tags **<login>** und **<password>** in den entsprechenden Abschnitten:

- Anmeldedaten des Plans – der Abschnitt **<plan><options><common_parameters>**
- Anmeldedaten zum Zugriff auf die gesicherten Daten – der Abschnitt **<plan><targets><inclusions>**
- Anmeldedaten zum Zugriff auf das Backup-Ziel – der Abschnitt **<plan><locations>**.

Seien Sie besonders vorsichtig bei der Modifikation des Tags **<password>**. Das Tag, das ein verschlüsseltes Kennwort enthält, sieht aus wie **<password encrypted="true">...</password>**.

So ändern Sie das verschlüsselte Kennwort

1. Starten Sie in der Befehlszeile das Utility **acronis_encrypt**.

   acronis_encrypt UserPassword#1

   (hier ist **UserPassword#1** das Kennwort, das Sie verschlüsseln wollen).
2. Das Utility gibt einen String aus, beispielsweise '**XXXYYYZZZ888**'.
3. Kopieren Sie diesen String und fügen Sie ihn folgendermaßen in das Tag ein:

   <password encrypted="true">XXXYYYZZZ888</password>

Das Utility **acronis_encrypt** ist auf jeder Maschine verfügbar, auf der die Acronis Backup Management Console oder das Befehlszeilenwerkzeug von Acronis Backup (**acrocmd**) installiert ist. Der Pfad zum Utility ist folgender:

- In einer 32-Bit-Version von Windows: **%CommonProgramFiles%\Acronis\Utils**
- In einer 64-Bit-Version von Windows: **%CommonProgramFiles(x86)%\Acronis\Utils**

- In Linux: **/usr/sbin**

Einen Backup-Plan die Anmeldedaten des Agenten verwenden lassen

Löschen Sie vor Importieren oder Bereitstellen der Exportdatei den Wert des benötigten Tags **<login>**. Der importierte oder verteilte Plan wird dann die Anmeldedaten des Agenten-Dienstes verwenden.

Beispiel

Finden Sie, damit der Backup-Plan unter den Anmeldedaten des Agenten läuft, das Tag **<login>** im Abschnitt **<plan><options><common_parameters>**. Das Tag sieht folgendermaßen aus:

```
<login>
   Administrator
</login>
<password encrypted="true">
   XXXYYYZZZ888
</password>
```

Löschen Sie den Wert des Tags **<login>**, damit das Tag folgendermaßen aussieht:

```
<login>
</login>
<password encrypted="true">
   XXXYYYZZZ888
</password>
```

So ändern Sie die Elemente für ein Backup

Austausch eines direkt spezifizierten Elements durch ein anderes, direkt spezifiziertes Element

Innerhalb des Abschnitts **<plan><targets><inclusions>**:

1. Löschen Sie das Tag **<ID>**.
2. Bearbeiten Sie den Wert des Tags **<Path>**, welches die Informationen über die zu sichernden Daten enthält; ersetzen Sie beispielsweise '**C:**' durch '**D:**'.

Austausch eines direkt spezifizierten Elements mit einem Auswahl-Template

Innerhalb des Abschnitts **<plan><options><specific><inclusion_rules>**:

1. Fügen Sie das Tag **<rules_type>** mit dem Wert '**disks**' oder '**files**' hinzu, abhängig vom Typ des von Ihnen benötigten Templates.
2. Fügen Sie das Tag **<rules>** hinzu.
3. Fügen Sie innerhalb des Tags **<rules>** den Eintrag **<rule>** mit dem benötigten Template hinzu. Das Template muss mit dem direkt spezifizierten Element korrespondieren. Falls das spezifizierte Element beispielsweise den Wert '**disks**' hat, dann können Sie die Templates **[SYSTEM]**, **[BOOT]** und **[Fixed Volumes]** verwenden; aber nicht die Templates **[All Files]** oder **[All Profiles Folder]**. Zu weiteren Informationen über Templates siehe 'Auswahlregeln für Volumes' und 'Auswahlregeln für Dateien und Ordner'.
4. Wiederholen Sie Schritt 3, um ein weiteres Template hinzuzufügen.

Beispiel

Das folgende Beispiel illustriert, wie Sie ein direkt spezifiziertes Element mit Auswahl-Templates ersetzen können.

Der ursprüngliche Abschnitt:

```
<specific>
   <backup_type>
      disks
   </backup_type>
   <disk_level_options />
   <file_level_options />
   <inclusion_rules />
<specific>
```

Der Abschnitt nach Anwendung der Auswahl-Templates:

```
<specific>
   <backup_type>
      disks
   </backup_type>
   <disk_level_options />
   <file_level_options />
   <inclusion_rules>
      <rules_type>
         disks
      </rules_type>
      <rules>
         <rule>
            [BOOT]
         </rule>
         <rule>
            [SYSTEM]
         </rule>
      </rules>
   </inclusion_rules>
<specific>
```

12.1.4 Deployment von Backup-Plänen als Dateien

Angenommen, Sie müssen ein und denselben Backup-Plan auf mehrere Maschinen anwenden. Eine gute Lösung ist es, den Backup-Plan von einer Maschine zu exportieren und ihn auf alle anderen Maschinen zu verteilen.

Die Funktionsweise

Auf jeder Maschine, auf der ein Agent installiert ist, gibt es einen dedizierten Ordner zum Speichern verteilter Pläne. Der Agent verfolgt Änderungen an diesem dedizierten Ordner. Sobald eine neue .xml-Datei im dedizierten Ordner erscheint, importiert der Agent den entsprechenden Backup-Plan aus dieser Datei. Falls Sie eine .xml-Datei im dedizierten Ordner ändern (oder löschen), ändert (oder löscht) der Agent auch automatisch den dazugehörigen Backup-Plan.

Die Exportdatei bearbeiten

Ein auf solche Art importierter Backup-Plan kann nicht über die grafische Benutzeroberfläche bearbeitet werden. Ein Bearbeiten der Exportdatei (S. 255) ist jedoch vor oder nach dem Deployment per Texteditor möglich.

Falls Sie die Datei vor dem Deployment bearbeiten, dann wirken sich die Änderungen bei allen Maschinen aus, auf die der Plan verteilt wird. Sie können auf Wunsch die direkte Spezifikation des zu sichernden Elementes ändern (beispielsweise C: oder C:\Users) – und zwar per Template (etwa [SYSTEM] oder [All Profiles Folder]). Zu weiteren Informationen über Templates siehe 'Auswahlregeln für Volumes' und 'Auswahlregeln für Dateien und Ordner'.

Sie können auf Wunsch auch die vom Plan verwendeten Anmeldedaten ändern.

So verteilen Sie einen Backup-Plan als Datei

1. Erstellen Sie auf einer der Maschinen einen Backup-Plan.
2. Exportieren Sie diesen als .xml-Datei (S. 254).
3. [Optional] Bearbeiten Sie die Exportdatei. Zu weiteren Informationen siehe 'Die Exportdatei bearbeiten (S. 255)'.
4. Verteilen Sie diese .xml-Datei zum dedizierten Ordner.

   Der Pfad des dedizierten Ordners

In Windows:

Der Standard-Pfad zum dedizierten Ordner ist **%ALLUSERSPROFILE%\Acronis\BackupAndRecovery\import** (für Windows Vista und späteren Versionen von Windows) oder **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\import** (für Windows-Versionen vor Windows Vista).

Der Pfad wird im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\Import\FolderPath** gespeichert.

Fehlt der Schlüssel, so bedeutet das, dass der Agent den dedizierten Ordner nicht überwacht.

Bearbeiten Sie diesen Schlüssel, um den Pfad zu ändern. Die Änderung wird erst nach einem Neustart des **Acronis Managed Machine Service** übernommen.

In Linux:

Der Standard-Pfad zum dedizierten Ordner ist **/usr/lib/Acronis/BackupAndRecovery/import**.

Der Pfad wird in der Datei **/etc/Acronis/MMS.config** gespeichert.

Bearbeiten Sie zur Änderung des Pfades den Wert **`/usr/lib/Acronis/BackupAndRecovery/import`** in folgendem Tag:

```
<key name="Import">
        <value name="FolderPath" type="TString">
               "/usr/lib/Acronis/BackupAndRecovery/import"
        </value>
</key>
```

Die Änderung wird erst nach einem Neustart des Agenten übernommen. Führen Sie folgenden Befehl als Benutzer 'root' aus, um den Agenten neu zu starten:

```
/etc/init.d/acronis_mms restart
```

Fehlt der Tag, so bedeutet das, dass der Agent den dedizierten Ordner nicht überwacht.

12.1.5 Backup-Plan-Details

Das Fenster **Backup-Plan-Details** (auch noch mal im Fensterbereich **Informationen** verfügbar) fasst alle Informationen zu einem ausgewählten Backup-Plan zusammen.

Falls die Ausführung des Plans einen Benutzereingriff erfordert, erscheint im oberen Bereich der Registerlaschen eine entsprechende Meldung. Die Nachricht enthält eine kurze Beschreibung des Problems und Aktionsschaltflächen, über die Sie die passende Aktion wählen oder den Plan stoppen können.

Details

Die Registerlasche **Backup-Pläne und Tasks** stellt folgende allgemeine Informationen über einen ausgewählten Plan zur Verfügung:

- **Name** – Bezeichnung des Backup-Plans
- **Ursprung** – ob der Plan direkt auf der Maschine erstellt wurde (lokaler Ursprung) oder vom Management Server auf der Maschine bereitgestellt wurde (zentraler Ursprung).
- **Ausführungsstadium** – Ausführungsstadium (S. 251) des Backup-Plans.
- **Status** – Status (S. 252) des Backup-Plans.
- **Maschine** – Name der Maschine, auf der der Backup-Plan existiert (nur für zentrale Backup-Pläne).
- **Planung** – ob der Task über eine Zeit-/Ereignisplanung verfügt oder auf manuellen Start gesetzt ist.
- **Letzte Startzeit** – wie viel Zeit seit dem letzten Plan- oder Task-Start verstrichen ist.
- **Deployment-Stadium** – die Deployment-Stadien des Backup-Plans (nur für zentrale Backup-Pläne).
- **Letzte Abschlusszeit** – wie viel Zeit seit der letzten Plan- oder Task-Fertigstellung verstrichen ist.
- **Letztes Ergebnis** – das Ergebnis der letzten Plan- oder Task-Ausführung.
- **Typ** – Typ des Backup-Plans oder Tasks.
- **Besitzer** – Name des Benutzers, der den Plan erstellt oder zuletzt modifiziert hat.
- **Nächste Startzeit** – wann der Plan oder Task das nächste Mal gestartet wird.
- **Kommentar** – Beschreibung des Plans (sofern verfügbar).

Tasks

In der Registerlasche **Tasks** wird eine Liste aller Tasks des gewählten Backup-Plans angezeigt. Klicken Sie auf **Details**, um sich Details zum gewählten Task anzeigen zu lassen.

Fortschritt

In der Registerlasche **Fortschritt** werden alle Aktivitäten eines gewählten Backup-Plans aufgelistet, die gerade ablaufen oder auf ihre Ausführung warten.

Verlauf

In der Registerlasche **Verlauf** können Sie den Verlauf aller vom Backup-Plan ausgeführten Aktivitäten untersuchen.

Backup-Quelle

Die Registerlasche **Quelle** stellt die folgenden Informationen über die zum Backup ausgewählten Daten zur Verfügung:

- **Quelltyp** – die Art der Daten, die zum Backup ausgewählt wurden
- **Elemente für das Backup** – die für die Sicherung ausgewählten Elemente und ihre Größe

Backup-Ziel

Die Registerlasche **Ziel** stellt die folgenden Informationen zur Verfügung:

- **Name** – Name des Archivs.
- **Speicherort** – Bezeichnung des Depots oder Pfad zu dem Verzeichnis, wo das Archiv gespeichert wird
- **Archiv-Kommentare** – Beschreibung zu einem Archiv (sofern vorhanden)
- **2.**, **3.**, **4.**, **5. Speicherort** – Namen der Speicherorte, zu denen das Archiv kopiert oder verschoben wurde (falls im Backup-Plan entsprechend konfiguriert).

Einstellungen

Die Registerlasche **Einstellungen** zeigt die folgenden Informationen:

- **Backup-Schema** – das gewählte Backup-Schema und all seine Einstellungen inkl. Planung
- **Validierung** – falls spezifiziert, Ereignisse vor oder nach Ausführung einer Validierung bzw. einer Validierungsplanung. Falls keine Validierung eingestellt wurde, wird der Wert **Nie** angezeigt.
- **Backup-Optionen** – gegenüber den Standardwerten veränderte Backup-Optionen

12.1.6 Task-/Aktivitätsdetails

Das Fenster **Task-/Aktivitätsdetails** (wird auch im Fensterbereich **Informationen** dupliziert) sammelt auf mehreren Registerlaschen alle Informationen über einen gewählten Task bzw. eine Aktivität.

Wenn ein Task oder eine Aktivität einen Benutzereingriff erfordert, dann erscheinen eine Meldung und Aktionsschaltflächen über den Registerlaschen. Die Meldung enthält eine kurze Beschreibung des Problems. Die Schaltflächen ermöglichen, den Task oder die Aktivität zu wiederholen oder zu stoppen.

12.2 Log

Das lokale Ereignis-Log speichert den Verlauf aller von Acronis Backup auf der Maschine durchgeführten Aktionen.

Wählen Sie zur Anzeige einer einfachen Liste von Log-Einträgen das Element **Ereignisse** aus dem Listenfeld **Anzeige** – um nach Aktivitäten gruppierte Log-Einträge angezeigt zu bekommen, wählen Sie **Aktivitäten**. Details zu einem ausgewählten Log-Eintrag oder einer Aktivität werden im Fensterbereich **Informationen** angezeigt (im unteren Teil der **Log**-Anzeige).

Verwenden Sie Filter, um gewünschte Aktivitäten und Log-Einträge in der Tabelle anzeigen zu lassen. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 18)'.

Wählen Sie eine Aktivität oder Log-Eintrag aus, um auf diese eine Aktion ausführen zu lassen. Zu Details siehe 'Aktionen für Log-Einträge (S. 260)' und 'Details zu Log-Einträgen (S. 262)'.

12.2.1 Aktionen für Log-Einträge

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Elemente in der Log-**Symbolleiste** ausgeführt. Diese Aktionen können außerdem über das Kontextmenü durchgeführt werden (indem Sie mit der rechten Maustaste auf den Log-Eintrag oder die Aktivität klicken).

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf Log-Einträge.

Aufgabe	Lösung
Eine einzelne Aktivität wählen	Wählen Sie **Aktivitäten** aus dem Listenfeld **Anzeige** und klicken Sie dann auf die gewünschte Aktivität. Im Fensterbereich **Informationen** werden für die gewählte Aktivität die Log-Einträge angezeigt.
Einen einzelnen Log-Eintrag wählen	Klicken Sie auf ihn.
Mehrere Log-Einträge wählen	▪ *Nicht zusammenhängend*: Halten Sie **Strg** gedrückt und klicken Sie nacheinander auf die gewünschten Log-Einträge ▪ *Zusammenhängend*: wählen Sie einen einzelnen Log-Eintrag, halten Sie dann die **Umschalt**-Taste gedrückt und klicken Sie auf einen weiteren Log-Eintrag. Darauf werden auch alle Log-Einträge zwischen der ersten und letzten Markierung ausgewählt.
Details zu einem Log-Eintrag einsehen	1. Wählen Sie einen Log-Eintrag. 2. Wählen Sie eine der nachfolgenden Varianten: ▪ Klicken Sie doppelt auf die Auswahl. ▪ Klicken Sie auf **Details**. Die Details des Log-Eintrags werden angezeigt. Zu Details über Aktionen für Log-Einträge siehe den Abschnitt 'Details zu Log-Einträgen'.
Gewählte Log-Einträge in eine Datei speichern	1. Lassen Sie die **Aktivitäten** anzeigen und wählen Sie die entsprechenden Aktivitäten oder lassen Sie die **Ereignisse** anzeigen und wählen Sie die entsprechenden Log-Einträge. 2. Klicken Sie auf **Auswahl in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge der gewählten Aktivitäten oder gewählten Log-Einträge werden in eine spezifizierte Datei gespeichert.
Alle Log-Einträge in eine Datei speichern	1. Stellen Sie sicher, dass keine Filter gesetzt sind. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge werden in die spezifizierte Datei gespeichert.
Alle gefilterten Log-Einträge in eine Datei speichern	1. Setzen Sie Filter, um eine Liste von Log-Einträgen zu erhalten, die den Filterkriterien entsprechen. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge in der Liste werden in die spezifizierte Datei gespeichert.
Alle Log-Einträge löschen	Klicken Sie auf **Alle Löschen**. Alle Einträge werden aus dem Log gelöscht und es wird ein neuer Log-Eintrag erstellt. Er enthält Informationen darüber, wer die Log-Einträge gelöscht hat und wann.

12.2.2 Details zu Log-Einträgen

Zeigt für den gewählten Log-Eintrag detaillierte Informationen an und erlaubt Ihnen, die Details in die Zwischenablage zu kopieren.

Um Details des nächsten oder vorherigen Log-Eintrages einsehen zu können, müssen Sie auf die Schaltfläche mit dem Pfeil nach unten bzw. oben klicken.

Klicken Sie auf die Schaltfläche **In Zwischenablage kopieren**, um die Details zu kopieren.

Datenfelder der Log-Einträge

Ein Log-Eintrag enthält folgende Datenfelder:

- **Typ** – Ereignistyp (Fehler, Warnung, Information).
- **Datum und Zeit** – Datum und Uhrzeit, wann das Ereignis stattfand.
- **Backup-Plan** – der Backup-Plan, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Task** – Der Task, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Code** – Kann leer sein oder dem Programmfehlercode entsprechen, wenn das Ereignis vom Typ „Fehler“ ist. Der Fehlercode ist eine Integer-Zahl, die vom Acronis-Support zum Lösen des Problems verwendet werden kann.
- **Modul** – Kann leer sein oder der Nummer des Programmmoduls entsprechen, bei dem das Ereignis aufgetreten ist. Es handelt sich um eine Integer-Zahl, die vom Acronis Support Service verwendet werden kann, um das Problem zu lösen.
- **Besitzer** – Der Benutzername des Backup-Plan-Besitzers (S. 23).
- **Nachricht** – Eine Textbeschreibung des Ereignisses.

Die Anzeige von Datum und Zeit variiert in Abhängigkeit von Ihren lokalen Einstellungen.

12.3 Alarmmeldungen

Ein Alarm ist eine Nachricht, die vor gegenwärtigen oder potentiellen Problemen warnt. In der Ansicht **Alarmmeldungen** können Sie die Probleme schnell identifizieren und lösen, indem Sie die aktuellen Alarmmeldungen überwachen und den Alarmverlauf einsehen.

Aktive und inaktive Alarmmeldungen

Ein Alarm kann sich entweder in einem aktiven oder inaktiven Stadium befinden. Ein aktives Stadium bedeutet, dass das Problem, welches den Alarm verursacht hat, immer noch existiert. Ein aktiver Alarm wird inaktiv, wenn das Problem, das den Alarm verursacht hat, entweder manuell oder von alleine gelöst wurde.

***Anmerkung**: Es gibt einen Alarmtyp, der immer aktiv ist: „Backup nicht erstellt“. Hintergrund ist, dass selbst bei erfolgreicher Behebung der Alarmursache und erfolgreicher Erstellung anderer, nachfolgender Backups, die Tatsache immer noch bestehen bleibt, dass das Backup nicht erstellt wurde.*

Probleme beheben, die Alarmmeldungen verursacht haben

Klicken Sie auf **Problem beheben**, um die Alarmursache herauszufinden und zu beseitigen. Sie werden daraufhin zur entsprechenden Ansicht geführt,wo Sie das Problem untersuchen und die notwendigen Schritte zu seiner Lösung durchführen können.

Sie können optional auch auf **Details anzeigen** klicken, um mehr Informationen über den von Ihnen gewählten Alarm zu erhalten.

Alarmmeldungen annehmen

Standardmäßig listet die Tabelle **Aktuelle Alarmmeldungen** sowohl aktive als auch inaktive Alarmmeldungen auf, solange bis diese nicht mehr akzeptiert werden. Um einen Alarm anzunehmen, wählen Sie diesen aus und klicken dann auf den Befehl **Annehmen**. Indem Sie einen Alarm annehmen, nehmen Sie ihn zur Kenntnis und übernehmen dieVerantwortung für ihn. Die angenommenen Alarmmeldungen werden dann ohne Änderung ihres Alarmstadiums zur Tabelle **Angenommene Alarmmeldungen** verschoben.

Die Tabelle **Angenommene Alarmmeldungen** speichert so einen Verlauf aller angenommenen Alarmmeldungen. Sie können hier herausfinden, wer einen Alarm angenommen hat und wann sich dieser ereignete. Angenommene Alarmmeldungen beider Stadien können aus der Tabelle entweder manuell entfernt werden – durch Verwendung der Schaltflächen **Löschen** und **Alle löschen** – oder automatisch entfernt werden (siehe „Alarmmeldungen konfigurieren" weiter unten in diesem Abschnitt).

Indem Sie auf **Alle in Datei speichern** klicken, können Sie den kompletten Tabelleninhalt in eine *.txt- oder *.csv-Datei exportieren.

Alarmmeldungen konfigurieren

Verwenden Sie zur Konfiguration von Alarmmeldungen folgende Optionen aus dem oberen Bereich der Anzeige **Alarmmeldungen**.

- **Alarmmeldungen anzeigen/verbergen** (S. 21) – spezifizieren Sie den Alarmtyp, der in der Ansicht **Alarmmeldungen** angezeigt werden soll.
- **Benachrichtigungen** (S. 267) – konfigurieren Sie die E-Mail-Benachrichtigungen über Alarmmeldungen.
- **Einstellungen** (S. 265) – spezifizieren Sie, ob inaktive Alarmmeldungen automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen; konfigurieren Sie, wie lange die angenommenen Alarmmeldungen in der Tabelle **Angenommene Alarmmeldungen** bewahrt werden sollen.

12.4 Eine Lizenz wechseln

Mit einem Lizenzwechsel schalten Sie ein Produkt vom Test- in den Vollversionsmodus um – oder Sie wechseln zu einem anderen Produkt. Die nachfolgende Tabelle fasst die verfügbaren Optionen zusammen.

Eine Lizenz wechseln	Warum er erforderlich sein kann
Testversion –> Vollversion	Sie haben nach dem Testen des Produktes entschieden, eine Lizenz zu kaufen.
Vollversion –> Vollversion, anderes Produkt	▪ Sie möchten ein Upgrade von Acronis Backup auf Acronis Backup Advanced durchführen, um die Möglichkeit zur zentralen Verwaltung zu nutzen. Weitere Informationen finden Sie im Abschnitt 'Ein Upgrade von Acronis Backup auf Acronis Backup Advanced durchführen' der Installationsanleitung. ▪ Sie haben eine Server-Lizenz (beispielsweise Acronis Backup für Windows Server) für eine Workstation verwendet. Sie wollen jetzt der Workstation eine Workstation-Lizenz zuweisen (Acronis Backup für PC). Sie können danach die Server-Lizenz widerrufen und sie für einen anderen Server verwenden.
Backups zum Cloud Storage* –> Vollversion	Sie haben nach der Erstellung von Backups zum bzw. in den Cloud Storage entschieden, dass Sie eine Lizenz mit mehr Funktionalität kaufen wollen.

Testversion –> Backups zum Cloud Storage*	Sie haben nach dem Test des Produktes entschieden, dass Sie nur Backups zum bzw. in den Cloud Storage durchführen wollen.

*Bevor Sie Backups zum bzw. in den Cloud Storage erstellen, müssen Sie auf den Maschinen, die Sie sichern wollen, ein Abonnement für den Cloud Backup Service aktivieren. Weitere Informationen finden Sie im Abschnitt 'Cloud Backup (S. 271)'.

So wechseln Sie eine Lizenz

1. Klicken Sie auf **Hilfe –> Lizenz wechseln**.
2. Klicken Sie neben Ihrer aktuellen Lizenz auf **Ändern** oder **Spezifizieren**, dann auf **Ändern** und abschließend auf **Folgende Lizenzschlüssel verwenden**.
3. Geben Sie den neuen Lizenzschlüssel ein.

Ein Cloud Backup-Abonnement verwalten

Der Block **Acronis Cloud** im Fenster **Lizenzen** erfordert es, dass Sie sich an Ihrem Acronis-Konto anmelden. Danach zeigt er das auf der Maschine aktivierte Cloud Backup-Abonnement an. Sollte kein Abonnement aktiviert sein, dann ermöglicht Ihnen dieser Block, ein Abonnement anzufordern, den nach dem Abonnementkauf erhaltenen Registrierungscode einzugeben und das Abonnement zu aktivieren.

12.5 Sammeln von Systeminformationen

Das Werkzeug zum Sammeln von Systeminformationen trägt Daten über die Maschine zusammen, mit der die Management Konsole verbunden ist, und speichert sie in einer Datei. Wenn Sie den technischen Support von Acronis kontaktieren, können Sie ihm diese Datei zur Verfügung stellen.

Diese Option ist bei bootfähigen Medien verfügbar und für Maschinen, auf denen der Agent für Windows oder ein Agent für Linux installiert ist.

So sammeln Sie Systeminformationen

1. Wählen Sie in der Management Konsole aus dem Hauptmenü **Hilfe** –> **Systeminformation von 'Maschinenname' sammeln**.
2. Spezifizieren Sie einen Speicherort für die Datei mit den Systeminformationen.

12.6 Die Maschinen-Optionen anpassen

Die Maschinen-Optionen definieren das allgemeine Verhalten von allen Acronis Backup-Agenten, die auf der verwalteten Maschine operieren und werden daher als spezifisch für die Maschine betrachtet.

Um auf die Maschinen-Optionen zuzugreifen, verbinden Sie die Konsole zur verwalteten Maschine und wählen dann im Menü **Optionen –> Maschinen-Optionen**.

12.6.1 Erweiterte Einstellungen

Spezifizieren Sie, was geschehen soll, wenn die Maschine bei einer Task-Ausführung heruntergefahren werden soll.

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Sie bestimmt das Verhalten von Acronis Backup, wenn das System herunterfährt. Dieses System-Herunterfahren tritt auf, wenn die Maschine ausgeschaltet oder neu gestartet wird.

Voreinstellung ist: **Laufende Tasks stoppen und herunterfahren.**

Falls Sie die Option **Laufende Tasks stoppen und herunterfahren** aktivieren, werden alle laufenden Tasks von Acronis Backup abgebrochen.

Falls Sie die Option **Auf Task-Abschluss warten** wählen, werden alle laufenden Tasks von Acronis Backup noch fertiggestellt.

12.6.2 Acronis Programm zur Kundenzufriedenheit (CEP)

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Diese Option legt fest, ob die Maschine am Acronis Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Falls Sie **Ja, ich möchte am CEP teilnehmen** aktivieren, werden auf der Maschine Informationen gesammelt (über die Hardware-Konfiguration, am häufigsten und am wenigsten verwendete Funktionen, sowie Probleme) und regelmäßig an Acronis geschickt. Die Ergebnisse sind dazu gedacht, Verbesserungen bei der Software und Funktionalität zu ermöglichen, um die Bedürfnisse von Acronis-Kunden noch besser zu erfüllen.

Acronis sammelt keine persönliche Daten. Lesen Sie die Teilnahmebedingungen auf der Acronis-Website oder in der Benutzeroberfläche des Produkts, um mehr über das CEP zu erfahren.

Die Option wird anfangs während der Installation des Acronis Backup-Agenten konfiguriert. Sie können diese Einstellung jederzeit in der Benutzeroberfläche des Programms ändern (**Optionen** –> **Maschinen-Optionen** –> **Programm zur Kundenzufriedenheit (CEP)**). Diese Option kann außerdem durch Verwendung der Gruppenrichtlinien-Infrastruktur konfiguriert werden. Eine per Gruppenrichtlinie definierte Einstellung kann nicht durch Verwendung der Programmoberfläche geändert werden, außer die Gruppenrichtlinie wird auf der Maschine deaktiviert.

12.6.3 Alarmmeldungen

12.6.3.1 Alarmverwaltung

Elemente von „Angenommene Alarmmeldungen" entfernen, wenn älter als

Diese Option definiert, ob Meldungen aus der Tabelle für **Angenommene Alarmmeldungen** gelöscht werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie für die angenommenen Alarmmeldungen einen Aufbewahrungszeitraum spezifizieren. Angenommene Alarmmeldungen, die älter als dieser Zeitraum sind, werden automatisch aus der Tabelle gelöscht.

Inaktive Alarmmeldungen automatisch zu „Angenommene Alarmmeldungen" verschieben

Diese Option definiert, ob alle Alarmmeldungen, die inaktiv werden, angenommen und automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie die Alarmtypen spezifizieren, auf die diese Option angewendet wird.

12.6.3.2 Zeit-basierte Alarmmeldungen

Letztes Backup

Die Option legt fest, ob eine Warnung erscheint, wenn auf der gegebenen Maschine nach Ablauf einer Zeitspanne kein Backup durchgeführt wurde. Sie können den Zeitraum einrichten, den Sie als kritisch für Ihr Geschäftsumfeld betrachten.

Voreinstellung ist: Warnen, wenn die letzte erfolgreiche Sicherung auf einer Maschine vor mehr als **5 Tagen** abgeschlossen wurde.

Der Alarm wird in der Ansicht **Alarmmeldungen** des Fensterbereichs **Navigation** angezeigt.

12.6.4 E-Mail-Einstellungen

Diese Option ermöglicht Ihnen E-Mail-Einstellungen zu konfigurieren, um Benachrichtigungen über Alarmmeldungen, die auf der verwalteten Maschine aufgetreten sind, zu versenden.

Die Benachrichtigungsplanungen und Arten der zu versendenden Alarmmeldungen werden unter **Maschinen-Optionen** –> **E-Mail-Einstellungen** –> **Alarmbenachrichtigungen** (S. 267) konfiguriert.

Voreinstellung ist: **Deaktiviert**.

Hinweis: *Alarmmeldungen warnen nur über Probleme. E-Mail-Benachrichtigungen über erfolgreiche Backup- und Recovery-Aktionen werden daher nicht versendet. Diese E-Mail-Benachrichtigungen werden unter Backup-Optionen –> Benachrichtigungen –> E-Mail (S. 96) bzw. unter Recovery-Optionen –> Benachrichtigungen –> E-Mail (S. 144) konfiguriert.*

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
2. Geben Sie in das Feld **Betreff** eine Beschreibung der Benachrichtigung ein oder lassen Sie den Wert leer. In dem Feld werden keine Variablen unterstützt.
3. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
4. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
5. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
6. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:
   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.
   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:

- **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
- **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
- **Benutzername** und **Kennwort** für den eingehenden Mail-Server.

d. Klicken Sie auf **OK**.

7. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

12.6.4.1 Alarmbenachrichtigungen

Diese Option ermöglicht Ihnen festzulegen, wann E-Mail-Benachrichtigungen über Alarmmeldungen, die auf der verwalteten Maschine aufgetreten sind, versendet werden sollen – und zudem festzulegen, welche Arten von Alarmmeldungen versendet werden sollen.

Stellen Sie bei Verwendung dieser Option sicher, dass die E-Mail-Benachrichtigungen unter **Maschinen-Optionen** –> **E-Mail-Einstellungen** (S. 266) korrekt konfiguriert sind.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie die Alarmbenachrichtigungen

1. Wählen Sie, wann die Alarmbenachrichtigungen versendet werden sollen:
   - **Sobald ein Alarm auftritt** – um eine Benachrichtigung jedes Mal zu versenden, wenn ein neuer Alarm auftritt.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.
   - **Benachrichtigung über alle aktuellen Alarmmeldungen nach Plan senden** – um eine gesammelte Alarmbenachrichtigung zu versenden, die alle Alarmmeldungen enthält, die in einer von Ihnen spezifizierten Zeitspanne aufgetreten sind.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.

     Konfigurieren Sie die **Frequenz** und **Zeit** der Benachrichtigung.
2. Klicken Sie auf **OK**.

12.6.5 Ereignisverfolgung

Es ist möglich, die von auf der verwalteten Maschine agierenden Agenten erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden. Wenn Sie die Optionen zur Ereignisverfolgung an keiner anderen Stelle außer dieser verändern, werden die Einstellungen für jeden lokalen Backup-Plan und jeden erstellten Task auf der Maschine wirksam.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

12.6.5.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup siehe „Unterstützung für SNMP (S. 34)“.

Voreinstellung ist: **Ausgeschaltet**.

Versenden von SNMP-Benachrichtigungen einrichten

1. Aktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.
2. Spezifizieren Sie die passenden Optionen wie folgt:
   - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
   - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
   - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

   Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Um die Funktion auszuschalten, deaktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.

Die Nachrichten werden über UDP verschickt.

Der nächste Abschnitt enthält zusätzliche Informationen über das Einstellen der SNMP-Dienste auf den empfangenden Maschinen (S. 268).

12.6.5.2 Einstellen der SNMP-Dienste auf der empfangenden Maschine

Windows

So installieren Sie den SNMP-Dienst auf einer Windows-Maschine:

1. **Start -> Systemsteuerung -> Software -> Windows-Komponenten hinzufügen/entfernen**
2. Wählen Sie **Verwaltungs- und Überwachungsprogramme.**
3. Klicken Sie auf **Details**.
4. Aktivieren Sie das Kontrollkästchen bei **SNMP (Simple Network Management Protocol)**.
5. Klicken Sie auf **OK**.

Sie sollten dann nach der Datei lmmib2.dll gefragt werden, die sich auf dem Installationsmedium des Betriebssystems befindet.

Linux

Um SNMP-Nachrichten auf einer Linux-Maschine zu empfangen, muss das Paket net-snmp (für RHEL und SUSE) oder das Paket snmpd (für Debian) installiert werden.

SNMP kann mit dem Befehl **snmpconf** konfiguriert werden. Die Standardkonfigurationsdateien befinden sich im Verzeichnis /usw/snmp:

- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Agenten
- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Trap Daemon.

12.6.5.3 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

Voreinstellung ist: **Ausgeschaltet**.

Wählen Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option einzuschalten.

Verwenden Sie das Kontrollkästchen **Ereignisse, die protokolliert werden**, um die Ereignisse zu filtern, die in der Ereignisanzeige von Windows aufgeführt werden:

- **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
- **Fehler und Warnungen**
- **Nur Fehler**.

Deaktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option auszuschalten.

12.6.6 Log-Bereinigungsregeln

Diese Option spezifiziert, wie das Log des Acronis Backup Agenten bereinigt wird.

Diese Option definiert die maximale Größe der Log-Datei des Agenten. Die Dateipfade sind wie folgt:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\events.db3**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\MMS\events.db3**.
- In Linux: **/var/lib/Acronis/BackupAndRecovery/MMS/events.db3**.

Voreinstellung ist: **Maximale Log-Größe: 50 MB**. **Bei Bereinigung 95% der maximalen Log-Größe bewahren**.

Wenn diese Option aktiviert ist, vergleicht das Programm nach jeweils 100 Log-Einträgen die tatsächliche Log-Größe mit der maximalen Größe. Sobald die maximale Log-Größe überschritten ist, löscht das Programm die ältesten Log-Einträge. Sie können bestimmen, wie viele Log-Einträge beibehalten werden sollen. Mit der Standardeinstellung 95% wird ein Großteil des Logs beibehalten. Mit der Minimaleinstellung 1% wird das Log fast vollständig geleert.

Diesen Parameter können Sie auch im Acronis Administrative Template setzen.

12.6.7 Cloud Backup Proxy

Diese Option ist nur wirksam, wenn Backup- und Recovery-Aktionen mit dem Acronis Cloud Storage über das Internet durchgeführt werden.

Diese Option bestimmt, ob der Acronis Agent die Internetverbindung über einen Proxy-Server herstellen soll.

Hinweis: *Der Proxy-Server muss so konfiguriert sein, dass er HTTP-/HTTPS- und TCP-Datenverkehr umleitet.*

So ändern Sie die Proxy-Server-Einstellungen

1. Aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**.
2. Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an – beispielsweise: **proxy.beispielname.com** oder **192.168.0.1**
3. Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers – beispielsweise: **80**
4. Sollte der Proxy-Server eine Authentifizierung benötigen, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.
5. Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

Wenn Sie die Proxy-Server-Einstellungen nicht kennen, bitten Sie Ihren Netzwerk-Administrator oder Internetdienstanbieter um Unterstützung.

Alternativ können Sie auch versuchen, diese Einstellungen aus der Konfiguration Ihres Webbrowsers zu entnehmen. Die nachfolgenden Befehle zeigen, wo Sie diese in drei populären Webbrowsern finden können.

- **Microsoft Internet Explorer:** Klicken Sie im Menü **Extras** auf den Befehl **Internetoptionen**. Klicken Sie in der Registerkarte **Verbindungen** auf den Befehl **LAN-Einstellungen**.
- **Mozilla Firefox.** Klicken Sie im Menü **Extras** auf den Befehl **Einstellungen** und dann auf **Erweitert**. Klicken Sie in der Registerkarte **Netzwerk**, im Bereich **Verbindung**, auf den Befehl **Einstellungen**.
- **Google Chrome.** Klicken Sie bei **Einstellungen** auf **Erweiterte Einstellungen anzeigen**. Und im Bereich **Netzwerk** dann auf **Proxy-Einstellungen ändern**.

13 Cloud Backup

Dieser Abschnitt vermittelt Details zur Verwendung von Acronis Cloud Backup. Dieser Dienst ermöglicht Ihnen, Ihre Daten per Backup zum bzw. in den Acronis Cloud Storage zu sichern.

Acronis Cloud Backup ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/cloud-backup/corporate

Um Backups zum bzw. in den Cloud Storage oder Wiederherstellungen aus dem Cloud Storage heraus einzurichten, folgen Sie den Schritten, die in den zugehörigen Abschnitten beschrieben sind:

Erstellung eines Backup-Plans (S. 38)

Erstellung eines zentralen Backup-Plans

Daten wiederherstellen (S. 112)

Der Hauptunterschied besteht darin, dass Sie den Cloud Storage als Backup-Ziel wählen.

13.1 Einführung in Acronis Cloud Backup

Dieser Abschnitt enthält eine kurze Übersicht über Acronis Cloud Backup und beantwortet Fragen, die möglicherweise während der Evaluierung oder Benutzung des Programms auftreten können.

13.1.1 Was ist Acronis Cloud Backup?

Acronis Cloud Backup ist ein Dienst, der Ihnen das Backup von Daten zum bzw. in den Acronis Cloud Storage ermöglicht. Um diese Dienstleistung zu nutzen, müssen Sie ein Abonnement erwerben, welches den für Backups reservierten Speicherplatz (die Storage Quota) festlegt sowie den Zeitraum für die Nutzung des Cloud Backup Services.

Beispiele für Abonnements:

- Ein Abonnement für mehrere Systeme vom Typ '1 TB/ 1 Jahr' bedeutet, dass Sie die Daten einer unbegrenzten Anzahl von physikalischen und/oder virtuellen Maschinen für den Zeitraum eines Jahres sichern können. Die Backups können nicht mehr als 1 Terabyte belegen.
- Ein 'Abonnement für PC' vom Typ '250 GB/1 Jahr' bedeutet, dass Sie die entsprechenden Daten von einer Maschine, deren Betriebssystem kein Windows-Server-Betriebssystem ist, für ein ganzes Jahr sichern können. Die Backups können nicht mehr als 250 GB belegen.

13.1.2 Was für Daten können gesichert und wiederhergestellt werden?

Sie können beliebige Dateien, Volumes oder die komplette physikalische Maschine so häufig wie gewünscht sichern. Anders als die meisten anderen Backup-Lösungen ermöglicht Acronis Cloud Backup auch direkt aus dem Cloud Storage heraus eine Wiederherstellung auf fabrikneue Computer. Einzelne Dateien können sowohl aus Laufwerk- wie auch aus Datei-Backups wiederhergestellt werden.

13.1.3 Wie lange werden Backups im Cloud Storage aufbewahrt?

Ihre Backups verbleiben im Cloud Storage, bis sie von Ihnen gelöscht werden oder das Abonnement abläuft. Eine Datenwiederherstellung aus dem Cloud Storage heraus ist bis zu 30 Tage nach Ablauf des Abonnements möglich.

Um den Speicherplatz des Online Storages effektiv nutzen zu können, haben Sie die Möglichkeit, die Aufbewahrungsregel '**Lösche Backups älter als**' einzustellen.

Beispiel

Für einen Datei-Server können Sie beispielsweise folgende Backup-Strategie verwenden.

Sichern Sie wichtige Dateien zweimal täglich per Planung. Stellen Sie die Aufbewahrungsregel „**Lösche Backups älter als**“ auf 7 Tage ein. Das bedeutet, dass die Software nach jeder Sicherung überprüft, ob es Backups gibt, die älter als 7 Tage sind und diese dann automatisch löscht.

Führen Sie bei einem Server die Backups des System-Volumes manuell aus (wenn erforderlich). Beispielsweise nachdem Sie Betriebssystem-Updates aufgespielt haben. Löschen Sie nicht mehr benötigte Backups manuell.

13.1.4 Wie sicher sind die Daten?

Backups können mit Hilfe des kryptographischen Algorithmus 'Advanced Encryption Standard' (AES) und eines frei gewählten Kennworts verschlüsselt werden. Das gewährleistet, dass keine andere Person auf Ihre Daten zugreifen kann.

13.1.5 Unterstützte Betriebssysteme und Virtualisierungsprodukte

Acronis Cloud Backup unterstützt die nachfolgenden Betriebssysteme und Virtualisierungsplattformen.

Server-Betriebssysteme

Windows

Windows 2000 SP4 – alle Editionen, mit Ausnahme der Datacenter und Professional Editionen

Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Server 2008 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)

Windows Small Business Server 2008

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation und Web Editionen

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – alle Editionen

Windows Server 2012/2012 R2 – alle Editionen

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2

Linux

Linux mit Kernel von 2.4.20 bis 3.12 und glibc 2.3.2 oder höher

Zahlreiche x86- und x86_64-Linux-Distributionen, einschließlich:

Red Hat Enterprise Linux 4.x, 5.x und 6.x

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04 und 13.10

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19 und 20

SUSE Linux Enterprise Server 10 und 11

Debian 4, 5, 6 und 7

CentOS 5.x und 6.x

Oracle Linux 5.x und 6.x – Unbreakable Enterprise Kernel und Red Hat Compatible Kernel

Bevor Sie das Produkt auf einem System installieren, das keinen RPM-Paketmanager verwendet (wie etwa ein Ubuntu-System), müssen Sie diesen Manager manuell installieren – beispielsweise durch Ausführung folgenden Befehls (als Benutzer 'root'): **`apt-get install rpm`**

Workstation-Betriebssysteme

Windows 2000 Professional SP4

Windows XP Professional SP2+ (x86, x64)

Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)

Windows 7 – alle Editionen mit Ausnahme der Starter und Home Editionen (x86, x64)

Windows 8/8.1 – alle Editionen mit Ausnahme der Windows RT-Editionen (x86, x64)

Virtualisierungsprodukte (Host-basiertes Backup von virtuellen Maschinen)

VMware ESX Infrastructure 3.5 Update 2+

VMware ESX(i) 4.0, 4.1, 5.0, 5.1 und 5.5

(Host-basierte Backups stehen nur für kommerzielle Lizenzen von VMware ESXi zur Verfügung).

Windows Server 2008 (x64) mit Hyper-V

Windows Server 2008 R2 mit Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 mit Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

13.1.6 FAQ zu Backup und Recovery

Dieser Abschnitt beantwortet typische Fragen zu Backup- und Recovery-Aktionen

13.1.6.1 Welche Backup-Methoden sind verfügbar?

Vollständige und inkrementelle Backup-Methoden stehen in mehreren Backup-Schemata zur Verfügung. Die erste Task-Ausführung produziert unabhängig vom jeweiligen Backup-Schema ein Voll-Backup; nachfolgende Task-Ausführungen erstellen dann inkrementelle Backups. Folgende Backup-Schemata stehen zur Verfügung:

- **Manueller Start** (verzögerter Start). Sie können den Task erneut manuell ausführen.
- **Einfach** (Start nach Planung). Sie können mit diesem Backup-Schema eine Aufbewahrungsregel zur automatischen Löschung alter Backups einstellen.

- **GVS (Großvater-Vater-Sohn)** (Start nach Planung). Sie spezifizieren, welche der täglichen Backups als wöchentliche und monatliche Backups betrachtet werden sollen. Sie können separate Aufbewahrungsregeln für tägliche, wöchentliche und monatliche Backups einrichten.
- **Türme von Hanoi** (Start nach Planung). Sie legen die Anzahl der Level fest. Dies ist die Anzahl der zu einem Zeitpunkt gespeicherten Backups. Überschüssige Backups werden so gelöscht, dass mehr Recovery-Punkte für jüngere und weniger für ältere Zeitpunkte übrigbleiben.
- Ein weiteres, nur für den Cloud Storage verfügbares Backup-Schema ist **Initial Seeding**. Mit diesem Schema startet das Backup sofort zu einem lokalen Zielspeicherort und verwendet die Voll-Backup-Methode. Um dieses Schema zu verwenden, benötigen Sie eine Initial Seeding (S. 57)-Lizenz.

13.1.6.2 Welche Recovery-Methoden sind verfügbar?

Es gibt zwei Methoden, wie Sie Ihre Daten vom bzw. aus dem Acronis Cloud Storage wiederherstellen können:

- Die Wiederherstellung von von Laufwerken oder Dateien unter Verwendung der Benutzeroberfläche oder Befehlszeilenschnittstelle von Acronis Backup. Mit dieser Methode können Sie im weiten Rahmen auf die Acronis Backup-Funktionalität zurückgreifen.
- Die Wiederherstellung von Dateien (S. 289) aus dateibasieren Backups unter Verwendung eines Webbrowsers. Zur Nutzung dieser Option benötigen Sie nur eine Maschine mit Internetzugang.

13.1.6.3 Ist der Cloud Storage auch von einem bootfähigen Acronis-Medium aus verfügbar?

Wiederherstellungen aus dem Acronis Cloud Storage sind möglich, Backups zum bzw. in den Storage dagegen nicht.

13.1.6.4 Kann Acronis Universal Restore verwendet werden, wenn eine Systemwiederherstellung aus dem Cloud Storage heraus erfolgt?

Ja. Acronis Universal Restore ist immer verfügbar, wenn Sie ein System aus dem Cloud Storage heraus wiederherstellen.

13.1.6.5 Was passiert, wenn während einer Cloud Backup- oder Recovery-Aktion die Netzwerkverbindung verloren geht?

Die Software wird alle 30 Sekunden versuchen, den Cloud Storage zu erreichen. Die Versuche werden aufgegeben, wenn die Verbindung entweder wieder aufgenommen wird – oder eine bestimmte Anzahl an Versuche durchgeführt wurde (je nachdem, was zuerst eintritt). Die Standardanzahl an Versuchen ist 300 bei Backups und 30 bei Wiederherstellungen.

Sie können die Zahl der Versuche und die Zeitspanne zwischen den Versuchen unter **Fehlerbehandlung** mit der Option **Bei Fehler erneut versuchen** ändern. Jeder Backup-Plan oder Recovery-Task enthält diese Option.

13.1.6.6 Was passiert, wenn Ihnen der Speicherplatz ausgeht?

Wenn die Backups einer Maschine den per Abonnement erlaubten Speicherplatz zu überschreiten drohen, erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie für zukünftige

Backups Speicherplatz freimachen müssen. Oder Sie könnten erwägen, die Storage-Quota zu erhöhen. Sie können auch eine Aufbewahrungsregel (S. 272) einstellen oder bearbeiten, damit zukünftig kein Überlauf mehr auftritt. Sobald der belegte Speicherplatz das Limit erreicht, verweigern die Backups ihre Ausführung.

13.1.6.7 Wofür ist der Bereinigungstask gedacht?

Jeder Backup-Plan mit gesetzter Bereinigungsregel enthält zusätzlich zum Backup-Task auch einen Bereinigungstask. Der Bereinigungstask durchsucht das auf Basis des Backup-Plans erstellte Archiv nach Backups, die ihre 'Lebensdauer' überschritten haben. Wenn solche Backups gefunden werden, bewirkt der Task deren Löschung im bzw. aus dem Cloud Storage. Da die Löschung auf Seiten des Cloud Storages durchgeführt wird, werden keine CPU-Ressourcen Ihrer Maschine beansprucht.

Der Bereinigungstask läuft nach jedem Cloud Backup, auch wenn das Backup selbst fehlgeschlagen ist. Zudem wird auch immer das letzte erfolgreiche Backup bewahrt. Weitere Informationen über die Aufbewahrungsregel finden Sie unter 'Wie lange werden Backups im Cloud Storage aufbewahrt? (S. 272)'.

Es ist normalerweise nicht notwendig, den Bereinigungstask manuell zu starten oder zu stoppen. Sie können dies jedoch in der Ansicht **Backup-Pläne und Tasks** tun.

13.1.6.8 Wie bewirken Sie, dass eine wiederhergestellte Maschine ihr Abonnement erkennt?

Wenn Sie eine physikalische Maschine aus einem Backup wiederherstellen, wird auch ein neuer 'Machine Identifier' erstellt. Daher kann die Maschine keine Backups zu dem Abonnement durchführen, das sie vor der Recovery-Aktion verwendet hat.

Um die Maschine zum selben Abonnement zu sichern, müssen Sie dieses der Maschine erneut zuweisen (S. 287). Wenn Sie dies tun, können die nächsten Backups der Maschine wieder inkrementell sein. Wenn Sie der Maschine ein neues Abonnement zuweisen, muss die Software ein neues Voll-Backup durchführen.

13.1.7 FAQ zu Initial Seeding

Dieser Abschnitt erklärt, was Initial Seeding ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

13.1.7.1 Was ist Initial Seeding?

Initial Seeding ist ein Extra-Service, bei dem Sie das initiale Voll-Backup lokal ausführen und dieses dann auf einer Festplatte (oder einem ähnlichen Laufwerk) an Acronis senden.

Acronis lädt das Backup dann zum bzw. in den Cloud Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Das Laufwerk erhalten Sie zurück, aber es ist nicht möglich, davon ein Recovery durchzuführen. Ein Recovery ist von einem lokal angeschlossenen Gerät jedoch mit der Option 'Large Scale Recovery (S. 281)' möglich.

13.1.7.2 Wann ist Initial Seeding sinnvoll?

Dieser Dienst hilft Ihnen, beim initialen Voll-Backup Zeit und Netzwerkverkehr zu sparen. Dies ist nützlich, wenn Sie sehr große Datenmengen oder komplette Maschinen im Cloud Storage sichern.

13.1.7.3 Ist Initial Seeding ein kostenpflichtiger Dienst?

Ja, Sie benötigen eine 'Initial Seeding'-Lizenz für jede Maschine.

13.1.7.4 Welche Laufwerkstypen können für Initial Seeding verwendet werden?

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: IDE, ATA, SATA sowie per USB angeschlossene Laufwerke. SCSI-Laufwerke werden nicht akzeptiert.

Sie können das Backup direkt auf das Gerät erstellen lassen – oder auf einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Gerät kopieren. Sorgen Sie dafür, dass das Gerät nur ein Volume hat und das Dateisystem NTFS oder FAT32 verwendet.

13.1.7.5 Kann mehr als ein Backup pro einzelner 'Initial Seeding'-Lizenz übermittelt werden?

Nein. Eine 'Initial Seeding'-Lizenz erlaubt Ihnen nur die Erstellung jeweils eines Backups auf der Maschine.

Sollten Sie jedoch einen Fehler gemacht haben oder aus irgendeinem Grund ein anderes Backup erstellen wollen, dann können Sie den 'Initial Seeding'-Auftrag auch abbrechen. Die Lizenz wird daraufhin wieder verfügbar.

13.1.7.6 Können Backups mehrerer Maschinen auf einem Laufwerk übermittelt werden?

Ja. Sie benötigen aber dennoch je eine Lizenz pro Maschine.

13.1.7.7 Wie kann eine Initial Seeding-Lizenz erworben werden?

Sie können eine Initial Seeding-Lizenz von einem Acronis-Partner oder im Acronis Online Store kaufen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Melden Sie sich an Ihrem Acronis-Konto an und geben Sie im Produktregistrierungsbereich den Registrierungscode ein. Die registrierte Lizenz erscheint auf Webseite mit Ihrer Kontoverwaltung in der Registerkarte **Initial Seeding / Recovery**.

Eine im Acronis Online Store erworbene Lizenz erscheint in der Registerkarte **Initial Seeding / Recovery** unmittelbar nach Abschluss des Zahlvorgangs.

13.1.7.8 Wie führe ich Initial Seeding aus?

1. Stellen Sie sicher, dass Sie ein Acronis Cloud Backup-Abonnement auf der Maschine aktiviert haben, für die Sie die Initial Seeding-Prodezur durchführen wollen (überspringen Sie diesen Schritt, falls Sie ein Abonnement für mehrere Systeme haben).

2. Falls Sie gerade ein Testabonnement verwenden, sollten Sie sicherstellen, dass Sie auch über ein bezahltes Abonnement verfügen und es der Maschine zugewiesen haben. Verwenden Sie den Initial Seeding Service nicht, wenn Sie kein bezahltes Abonnement haben.
3. Entscheiden Sie sich für das Medium (S. 276), welches Sie für den Versand verwenden wollen.
4. Schließen Sie das Medium bzw. Laufwerk an die Maschine an, die Sie per Backup sichern wollen. Alternativ können Sie das Backup auch zu einem lokalen Ordner oder einer Netzwerkfreigabe sichern – und es anschließend dann auf das Medium kopieren/verschieben.
5. Starten Sie Acronis Backup, klicken Sie auf **Backup-Plan erstellen** und erstellen Sie auf dieser Maschine einen Backup-Plan:
   - Wählen Sie bei **Backup-Quelle** die Laufwerke/Volumes oder Dateien/Ordner, die Sie sichern wollen.
   - Spezifizieren Sie den **Cloud Storage** als **Backup-Ziel**.
   - Wählen Sie bei **Backup-Schema** die Einstellung **Initial Seeding**. Spezifizieren Sie das besprochene Medium als Backup-Ziel.
   - [Optional, aber dringend empfohlen] Aktivieren Sie unter **Backup-Optionen** –> **Schutz des Archivs** eine Verschlüsselung für das Backup.

   Das Backup startet unmittelbar, sobald Sie abschließend auf **OK** klicken.
6. [Optional] Wenn Sie Backups von einer anderen Maschine hinzufügen wollen, dann schließen Sie das Medium an diese Maschine an und wiederholen Sie die entsprechenden Schritte. Sie benötigen für jede Maschine, die Sie per Backup sichern wollen, eine separate Initial Seeding-Lizenz.
7. Verpacken (S. 277) Sie das Medium zusammen mit einem frankierten Rücksendeetikett und senden Sie es über den herkömmlichen Postweg an Acronis. Sie finden die Adresse auf der Webseite zur Kontoverwaltung unter **Initial Seeding / Recovery** –> **Laufende Aufträge** –> **Initial Seeding-Aufträge** –> **Datacenter-Adresse**.
8. Kennzeichnen Sie auf derselben Webseite den Auftrag als 'Versendet' und verfolgen (S. 280) Sie den Auftragsstatus.
9. Sobald Sie sehen, dass das Backup zum bzw. in den Cloud Storage hochgeladen wurde, können Sie den Backup-Plan so bearbeiten, dass inkrementelle Backups erstellt werden.
   - Wählen Sie bei **Backup-Schema** das gewünschte Backup-Schema und spezifizieren Sie dessen Einstellungen.
   - Klicken Sie auf **Speichern**.

   Ihr Backup-Plan wird bei einem manuellen oder geplanten Start dem bereits im Cloud Storage gespeicherten anfänglichen Backup weitere inkrementelle Backups hinzufügen.

13.1.7.9 Wie verpacken Sie ein Laufwerk zur Versendung richtig?

Es ist sehr wichtig, dass Sie Ihre Festplatte (oder ein ähnliches Laufwerk) sorgfältig für den Versand verpacken. Durch eine gute Verpackung schützen Sie Ihr Laufwerk vor Transportschäden.

Laufwerkstypen

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: Per IDE, ATA, SATA sowie USB anschließbare Laufwerke.

SCSI-Laufwerke werden nicht akzeptiert.

Verpackung

Verwenden Sie – sofern möglich/verfügbar – die Originalverpackung des Laufwerks. Anderenfalls können Sie geeignetes Verpackungsmaterial auch bei entsprechenden Poststationen oder ähnlichen Geschäften erhalten. Sie sollten dem Laufwerk außerdem alle benötigten Kabel und Adapter beilegen. Acronis kann Ihre 'Initial Seeding'-Anforderung nicht bearbeiten, falls der Sendung keine passenden Kabel beiliegen.

Nachfolgend finden Sie Hinweise zur geeigneten Verpackung Ihres Laufwerks.

Schritt 1

Entfernen Sie Ihr Laufwerk vorsichtig von der entsprechenden Maschine.



Schritt 2

Stecken Sie das Laufwerk in eine Antistatikhülle, um es vor elektrostatischen Entladungen zu schützen. Falls Sie keine Antistatikhülle zur Verfügung haben, können Sie das Laufwerk alternativ auch mit Alufolie umwickeln.

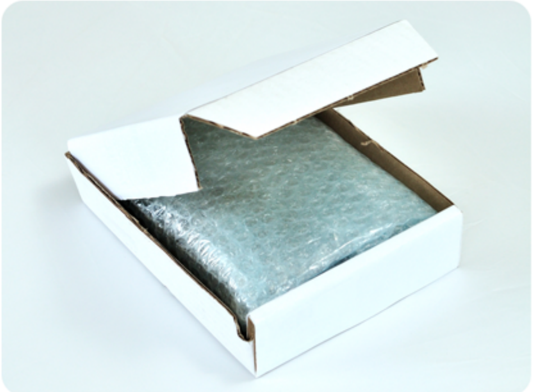


Schritt 3

Verwenden Sie eine stabile Box, die mindestens doppelt so groß wie das Laufwerk ist. Wickeln Sie das Laufwerk über alle 6 Seiten mit einer Luftpolsterfolie so ein, dass es genau in die Box passt und sich in dieser nicht bewegen kann.

*Verwenden Sie **keine** Styropor-**Chips** zur Verpackung, da diese nicht genügend Schutz bieten.*
*Versenden Sie das Laufwerk **nicht** einfach in einer herkömmlichen **gepolsterten Versandtasche**.*





Schritt 4

Wählen Sie den von Ihnen gewünschten Paketdienst für den Versand. Erstellen bzw. bedrucken Sie (z.B. über eine entsprechende Website des Paketdienstes) zwei bereits frankierte Versandetiketten:

1. Das **Versandetikett zur Hinsendung** Ihres Laufwerks. Dieses Etikett gehört auf die Oberseite der Box. Sie müssen das Paket dann an ein Acronis Datacenter versenden. Die Adresse des entsprechenden Datacenters finden Sie auf der Webseite zur Kontenverwaltung innerhalb der Registerlasche **Initial Seeding/Recovery** (indem Sie auf den Befehl **Datacenter-Adresse** klicken).

   Falls Sie möglichst schnell mit der Erstellung inkrementeller Backups beginnen wollen, sollten Sie erwägen, einen Express- bzw. Nachtversanddienst zu verwenden. Sobald die Daten beim Datacenter eingetroffen sind, stehen Sie üblicherweise am darauf folgenden Arbeitstag zur Verfügung.
2. Das **Versandetikett zur Rücksendung** Ihres Laufwerks. Legen Sie dieses Etikett in die Box zum Laufwerk. Zur Rücksendung wird dieselbe Verpackung verwendet (sofern sie nicht beschädigt wurde). Wenn Sie Ihrer Sendung kein frankiertes Etikett beilegen, wird Ihr Laufwerk **sicher entsorgt**.

   Sie können zur Rücksendung Ihres Laufwerks eine kostengünstige Methode bzw. einen Paketdienst Ihrer Wahl verwenden.



Schritt 5

Versiegeln Sie die Box sicher mit einem stabilen Klebeband. Kleben Sie dann das **Versandetikett zur Hinsendung** Ihres Laufwerks auf die Oberseite der Box und achten Sie darauf, dass das Etikett nicht über eine der Kanten geklebt ist.



13.1.7.10 Wie kann der Auftragsstatus für Initial Seeding verfolgt werden?

Auf der Acronis-Website zeigt die Registerkarte **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für jede Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Das Backup ist bereit für den Start und die Lizenz kann weder für dieselbe, noch eine andere Maschine erneut verwendet werden. Sie können von hier an den Auftrag aber noch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Ein Voll-Backup wurde gestartet** – Dieser Zustand wird eingestellt, wenn das erste Backup ausgeführt wird. Ab diesem Moment beginnt die Laufzeit des Vertrags.
- **Ein Voll-Backup wurde erfolgreich abgeschlossen** – Das Backup wurde fertig gestellt und der Auftrag ist bereit zur Versendung. Sie können das Medium jetzt verschicken:

  Schritt 1. Verpacken Sie das Medium gemäß der Anleitung für Verpackung und Versand des Laufwerks (S. 277), um Transportschäden zu vermeiden. Falls Sie wollen, dass das Medium nach dem Upload der Daten an Sie zurückgeschickt wird, legen Sie der Verpackung neben dem Laufwerk auch ein vorbereitetes, ausreichend frankiertes Rücksendeetikett bei.

  Schritt 2. Verschicken Sie das Laufwerk mit dem von Ihnen gewünschten Paketdienst zum Acronis Datacenter.

  Schritt 3. Teilen Sie uns den Versand des Pakets mit, indem Sie Ihren Auftrag als „Versendet“ kennzeichnen.

  Sie erhalten eine Benachrichtigung, sobald Acronis den Auftrag erhalten hat und sobald der Auftrag abgeschlossen wurde. Sofern erforderlich, werden Sie von Acronis während der Auftragsbearbeitung kontaktiert.
- [Gelegentlich] **Fehler bei Backup-Erstellung** – Während der Sicherung ist ein Fehler aufgetreten. Überprüfen Sie die Parameter des Backup-Plans und versuchen Sie es dann erneut.
- **Das Medium wurde versendet** – Dieser Status wird eingestellt, nachdem Sie den Auftrag mit „Versendet“ gekennzeichnet haben.

- **Das Medium wurde von Acronis erhalten** – Acronis hat mit der Bearbeitung Ihres Auftrages begonnen. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen. Die Erstellung eines neuen Initial Seeding-Backups erfordert eine neue Initial Seeding-Lizenz.
- **Der Upload der Daten wurde gestartet** – Das Upload der Daten zum bzw. in den Acronis Cloud Storage hat begonnen.
- **Der Upload der Daten wurde abgeschlossen** – Das anfängliche Voll-Backup wurde erfolgreich zum bzw. in den Cloud Storage hochgeladen. Sie können nun inkrementelle Cloud Backups durchführen.
- **Der Auftrag wurde ausgeführt. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Das Medium wurde zurückgeschickt (Paketdienst und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Auftragsbearbeitung unterbrochen. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde noch vor Versendung des Mediums abgebrochen, dessen Rücksendung ist daher nicht erforderlich.
- [Gelegentlich] **Der Auftrag wurde abgebrochen. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Der Auftrag wurde abgebrochen, während das Medium im Datacenter war. Das Medium wurde zurückgeschickt (Paketdienst und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.

13.1.8 FAQ zu Large Scale Recovery

Dieser Abschnitt erklärt, was Large Scale Recovery ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

13.1.8.1 Was ist Large Scale Recovery?

Large Scale Recovery ist ein Extra-Service, mit dem Sie eine Kopie der Backups erhalten, welche sich im Cloud Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Sobald Sie ein Large Scale Recovery für eine bestimmte Maschine ordern, sendet Acronis Ihnen ein USB-Laufwerk mit allen Backups, die Sie von dieser Maschine erstellt haben. Sie können die Daten direkt vom Laufwerk wiederherstellen oder die Backups zu einem lokalen oder Netzwerkordner kopieren.

13.1.8.2 Wann ist Large Scale Recovery sinnvoll?

Der Dienst hilft Zeit und Netzwerkverkehr zu sparen, beispielsweise im Desasterfall, bei Wiederherstellung großer Datenmengen oder kompletter Maschinen. Eine Wiederherstellung von Daten im Bereich vieler Hundert Gigabytes über das Internet kann Tage dauern. Dieser Prozess ermöglicht Ihnen eine schnellere Wiederherstellung.

13.1.8.3 Muss Initial Seeding zur Nutzung von Large Scale Recovery ausgeführt werden?

Nein, diese Dienstleistungen sind voneinander unabhängig.

13.1.8.4 Ist Large Scale Recovery kostenpflichtig?

Ja, Sie benötigen je eine Lizenz für Large Scale Recovery pro Maschine. Durch diese Lizenz wird Ihnen bei Bedarf ein Laufwerk zugeschickt, das alle aktuell verfügbaren Backups dieser Maschine enthält. Um auch zukünftige Backups zu erhalten, benötigen Sie eine neue 'Large Scale Recovery'-Lizenz.

13.1.8.5 Kann ein Large Scale Recovery auf einer anderen Maschine erfolgen?

Ja. Sie können Ihre Daten beliebig oft auf jeder gewünschten Maschine wiederherstellen. Acronis Universal Restore ist bereits integriert, so dass Sie ein Betriebssystem auch auf abweichender Hardware wiederherstellen können.

13.1.8.6 Können Backups mehrerer Maschinen gemeinsam auf einem Laufwerk zurückerhalten werden?

Nein. Es ist ein separates Laufwerk für jede Maschine erforderlich.

13.1.8.7 Wie kann eine 'Large Scale Recovery'-Lizenz erworben werden?

Sie können eine 'Large Scale Recovery'-Lizenz von einem Acronis-Partner oder im Acronis Online Store kaufen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Melden Sie sich an Ihrem Acronis-Konto an und geben Sie im Produktregistrierungsbereich den Registrierungscode ein. Die registrierte Lizenz erscheint auf Webseite mit Ihrer Kontoverwaltung in der Registerkarte **Initial Seeding / Recovery**.

Eine im Acronis Online Store erworbene Lizenz erscheint in der Registerkarte **Initial Seeding / Recovery** unmittelbar nach Abschluss des Zahlvorgangs.

13.1.8.8 Wie kann der Auftragsstatus für Large Scale Recovery verfolgt werden?

Auf der Acronis-Website zeigt die Registerlasche **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für eine beliebige Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Dieser Status ist nach Auftragsabschluss für Large Scale Recovery eingestellt. Diese Lizenz kann nicht mehr für eine andere Maschine verwendet werden. Sie können von diesem Punkt an den Auftrag auch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Der Auftrag wird bearbeitet** – Das Data Center hat mit der Auftragsbearbeitung begonnen.
- **Schreibe Daten** – Ihre Backups werden gerade auf das Medium geschrieben. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen.
- **Schreiben der Daten wurde abgeschlossen** – Ihre Backups wurden erfolgreich auf das Medium geschrieben.
- **Bereit, das Medium zu versenden** – Ihr Auftrag wurde bearbeitet und das Medium wird in Kürze verschickt.

- **Der Auftrag wurde ausgeführt. Das Medium wurde versendet** – Das Medium wurde an Sie verschickt (Transportunternehmen und Sendeverfolgungsnummer sind angegeben).
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Bearbeitung des Auftrages pausiert. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde abgebrochen.
- [Gelegentlich] **Adresse ist nicht zustellbar** – Acronis kann das Laufwerk nicht verschicken. Klicken Sie auf der gleichen Webseite auf **Meine Lieferadresse ändern** und spezifizieren Sie die richtige Adresse für den Auftrag.
- [Gelegentlich] **Adresse wurde aktualisiert** – Dieser Status wird eingestellt, nachdem Sie die Zustelladresse auf der Acronis-Website geändert haben.

13.1.8.9 Wie wird Large Scale Recovery ausgeführt?

Der Recovery-Vorgang ist identisch zu Wiederherstellungen, die aus dem Cloud Storage heraus erfolgen. Sie spezifizieren lediglich den Pfad zum Speicherort Ihrer Backups. Weitere, detaillierte Informationen zu Recovery-Aktionen finden Sie in der kontextabhängigen Hilfe.

13.1.9 FAQ zum Abonnement-Lebenszyklus

Dieser Abschnitt erläutert den Lebenszyklus eines Abonnement und die Aktionen mit Abonnements, die Sie auf der Webseite zur Kontonverwaltung ausführen können.

13.1.9.1 Wie greife ich auf meine Webseite zur Kontoverwaltung zu?

Gehen Sie zu http://www.acronis.de/my/cloud-backup/corporate und melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie nicht registriert sind).

So gelangen Sie von Acronis Backup ausgehend auf die entsprechende Webseite:

1. Klicken Sie im Menü **Aktionen** auf **Backup jetzt** oder **Backup-Plan erstellen**.
2. Klicken Sie auf **Speicherort** und dann auf **Abonnements erwerben oder verwalten**.
3. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie bisher noch nicht registriert sind).

13.1.9.2 Wo sind erworbene Abonnements zu finden?

Wenn Sie Abonnements von einem Acronis-Partner erworben haben, sollten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jedes Abonnement erhalten haben. Gehen Sie zur Kontoverwaltungs-Webseite, klicken Sie auf **Neuen Registrierungscode eingeben** und geben Sie dann die Registrierungscodes ein. Diese Abonnements werden in der Registerlasche **Abonnements verwalten** in der Liste der verfügbaren Abonnements angezeigt.

Abonnements, die über die Acronis-Website erworben wurden, werden unmittelbar danach in dieser Registerkarte angezeigt.

13.1.9.3 Wann beginnt ein Abonnement?

Bei Abonnements **für mehrere Systeme** beginnt der Abonnementzeitraum mit dem Tag des Erwerbs.

Bei Abonnements **pro System** beginnt der Abonnementzeitraum, sobald ein Abonnement auf der Maschine aktiviert wurde.

13.1.9.4 Was passiert bei Ablauf eines Abonnements?

Einen Monat vor Ablaufdatum des Abonnements erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie das Abonnement erneuern (S. 284) müssen, um mit den Backups der Maschine fortfahren zu können.

Falls Sie das Abonnement nicht erneuern, können Sie Daten noch für weitere fünf Tage nach dem Ablaufdatum zum bzw. in den Cloud Storage sichern. Sie können Daten aus dem Cloud Storage heraus noch bis zu 30 Tage nach dem Ablaufdatum wiederherstellen.

13.1.9.5 Wie wird ein Abonnement erneuert?

Erwerben Sie ein anderes Abonnement und spezifizieren Sie dieses als nächstes Abonnement für die Maschine. Das neue Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Ein abgelaufenes Abonnement kann innerhalb von fünf Tagen nach Ablauf erneuert werden. In solchen Fällen wird das neue Abonnement unverzüglich aktiviert.

Ein einzelnes Abonnement erneuern

Sie können ein aktiviertes Abonnement erneuern – und zwar zu einem Abonnement mit der gleichen oder einer größeren Storage-Quota.

Um ein Abonnement **für mehrere Systeme** zu erneuern, benötigen Sie ebenfalls ein Abonnement für mehrere Systeme. Um ein Abonnement **pro System** zu erneuern, benötigen Sie ein Abonnement pro System desselben Typs oder ein Abonnement **für mehrere Systeme**.

Ein Abonnement für **virtuelle Maschinen** (jetzt verworfen) kann zu einem **Server**-Abonnement erneuert werden.

Abonnements für mehrere Systeme

Um ein Abonnement für **mehrere Systeme** erneuern zu können, müssen Sie zur Kontoverwaltungs-Webseite gehen, dort neben dem Abonnement für mehrere Systeme auf **Erneuern** klicken – und dann den Anweisungen auf dem Bildschirm folgen.

Das neue Ablaufdatum erscheint in der Spalte **Verfällt**.

- Falls das neue Abonnement dieselbe Storage-Quota wie das alte hat, werden die Abonnementzeiträume zusammengefügt.
- Falls das neue Abonnement eine größere Storage-Quota hat, wird der resultierende Abonnementzeitraum wie im Abschnitt 'Wie kann die Storage-Quota für eine Maschine erhöht werden?' beschrieben berechnet.

Abonnements pro System

Um ein Abonnement für **pro Systeme** erneuern zu können, müssen Sie zur Kontoverwaltungs-Webseite gehen, dort die Maschine suchen, für die Sie das Abonnement erneuern wollen, dann neben dieser Maschine auf **Erneuern** klicken – und schließlich den Anweisungen auf dem Bildschirm folgen.

Das neue Abonnement erscheint für die Maschine in der Spalte **Nächstes Abonnement**.

Mehrere aktivierte Abonnements auf einmal erneuern

Diese Aktion ist möglich, wenn die Anzahl der neuen Abonnements mit der Zahl der gegenwärtig genutzten Abonnements übereinstimmt.

Sorgen Sie dafür, dass die neuen Abonnements auf der Webseite zur Kontoverwaltung verfügbar sind. Klicken Sie dann auf **Alle erneuern**. Das Bestätigungsfenster fasst zusammen, welche Abonnements erneuert werden. Wenn für einige Maschinen keine identischen Abonnements gefunden werden, haben Sie die Option, den automatischen Vorgang abzubrechen und jedes Abonnement einzeln zu erneuern.

Was bedeutet „Automatisches Erneuern"?

Wenn ein Abonnement endet, wird das nächste Abonnement automatisch aus den verfügbaren Abonnements gewählt, also automatisch erneuert. Das nächste Abonnement muss zum aktuellen Abonnement identisch sein.

Wenn kein identisches Abonnement gefunden wird, erfolgt keine automatische Erneuerung und die Backups könnten fehlschlagen. Es werden keine Abonnements automatisch gekauft. Es können nur Abonnements verwendet werden, die zum Zeitpunkt der automatischen Erneuerung verfügbar sind. Sie können die automatische Erneuerung für jedes einzelne Abonnement wählen oder als Aktion für alle vorhandenen, aktivierten Abonnements.

13.1.9.6 Wofür gibt es die Spalte „Gruppe"?

Damit können Sie solche Aktionen wie **Alle erneuern** oder **Alle automatisch erneuern** auf ausgewählte Abonnements anwenden. Spezifizieren Sie den gewünschten Gruppennamen (beispielsweise Verkaufsabteilung), bei den Abonnements, die Sie gruppieren wollen. Klicken Sie auf den Spaltenkopf **Gruppe**, um die Abonnements zu sortieren und wenden Sie dann die gewünschten Aktionen auf die Gruppe an.

13.1.9.7 Kann ein Abonnement auf einer Maschine widerrufen werden?

Sie können ein einmal aktiviertes Abonnement nicht erneut in die Liste der verfügbaren Abonnements stellen, aber sie können es einer beliebigen Maschine über die Benutzeroberfläche von Acronis Backup neu zuweisen (S. 287).

13.1.9.8 Können Abonnements gekündigt werden?

Warten Sie einfach, bis das Abonnement abgelaufen ist. Rückerstattungen sind bei Abonnements für Cloud Backup nicht möglich.

13.2 Was sind meine ersten Schritte?

Gehen Sie zu http://www.acronis.de/my/cloud-backup/corporate und melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie nicht registriert sind). Dies ist die *Webseite zur Kontoverwaltung*. Sie können hier ein Test-Abonnement erhalten, einen Acronis-Partner finden oder ein Abonnement online kaufen. Neu erhaltene Abonnements sind als verfügbare Abonnements in der Registerkarte **Abonnements verwalten** aufgelistet.

Wenn Sie Ihre Abonnements von einem Acronis-Partner erworben haben, dann registrieren Sie diese manuell unter Verwendung des Links '**Neuen Registrierungscode eingeben**'. Der Registrierungscode kommt zusammen mit der Kaufbestätigung per E-Mail.

Installieren Sie als Nächstes die Acronis-Software (falls diese noch nicht installiert wurde) – und aktivieren (S. 287) Sie die Abonnements auf denjenigen Maschinen, die Sie per Backup sichern wollen. Sie können anschließend mit dem Backup zum bzw. in den Acronis Cloud Storage beginnen.

13.3 Abonnement wählen

Abonnements für mehrere Systeme

Ein Abonnement für **mehrere Systeme** ermöglicht Ihnen, eine unbegrenzte Anzahl von Maschinen zu sichern. Alle gesicherten Maschinen teilen sich eine gemeinsame Storage-Quota. Der Abonnementzeitraum beginnt mit dem Tag des Erwerbs.

Abonnements pro System

Ein Abonnement **pro System** ermöglicht Ihnen, eine einzelne Maschine per Backup zu sichern. Die Storage-Quota gilt nur für diese Maschine. Der Abonnementzeitraum beginnt, sobald das Abonnement auf der Maschine aktiviert wurde.

Wählen Sie, abhängig vom auf der Maschine laufenden Windows-Betriebssystem, den Abonnementtyp **Server** oder **PC**. Falls Sie im Zweifel sind, ob es sich bei der Maschine um einen Server oder eine Workstation handelt, dann informieren Sie sich in der Liste der unterstützten Betriebssysteme (S. 272).

Wenn es sich abzeichnet, dass Ihre Backups in der Summe größer als die Storage-Quota für das Abonnement sein werden, können Sie ein Server-Abonnement auch auf einer Workstation verwenden. Die umgekehrte Verwendung ist jedoch nicht möglich. Sie können einen Server nicht mit einem Abonnement für PCs sichern.

Test-Abonnements

Sie können ein freies Abonnement **pro System** für je ein Konto erhalten. Die Storage-Quota des Testabonnements entspricht der des Standardabonnements. Der Abonnementzeitraum ist auf einen Monate beschränkt.

Ein Test-Abonnement zu erhalten ist solange möglich, bis Sie ein bezahltes Abonnement eingehen. Sie können ein Test-Abonnement zusammen mit bezahlten Abonnements verwenden. Für Test-Abonnements gelten die gleichen Ablaufregeln wie für bezahlte Abonnements.

Sie können den Dienst nach Ablauf des Testabonnements weiter verwenden, wenn Sie ein Abonnement **pro System** desselben Typs oder ein Abonnement **für mehrere Systeme** erwerben – und dann das Test-Abonnement erneuern, indem Sie das gekaufte Abonnement spezifizieren. Die auf per Backup gesicherten Daten bleiben erhalten. Regelmäßige Backups Ihrer Maschinen werden unterbrechungsfrei fortgesetzt. Ein erneutes Voll-Backup ist nicht nötig.

Gehen Sie folgendermaßen vor, um ein Test-Abonnement zu erhalten:

- Klicken Sie auf der Webseite zur Kontoverwaltung auf den Link zum Testen von Cloud Backup – und wählen Sie dann den benötigten Abonnementtyp.
- Installieren Sie Acronis Backup auf der zu sichernden Maschine, starten Sie das Produkt, klicken Sie auf **Backup jetzt** oder **Backup-Plan erstellen**, klicken Sie auf **Speicherort** und dann auf **Test-Abonnement erhalten**. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind). Es wird automatisch ein Test-Abonnement erstellt und der Maschine zugewiesen.

13.4 Cloud Backup-Abonnements aktivieren

Ein Abonnement auf einer Maschine zu aktivieren, bedeutet, der Maschine zu erlauben, Backups zum bzw. in den Cloud Storage zu erstellen.

Ein Abonnement **für mehrere Systeme** wird automatisch aktiviert, sobald Sie damit beginnen, Backups der Maschine zum bzw. in den Acronis Cloud Storage zu erstellen.

Ein Abonnement **pro System** (für PCs oder Server) muss manuell aktiviert werden. Der entsprechende Abonnementzeitraum beginnt mit dem Augenblick der Aktivierung.

Wichtig! *– Bevor Sie das* erste *Abonnement für Ihr Konto aktivieren, sollten Sie das in Ihrem Profil ausgewählte Land überprüfen. Der Dienst bestimmt abhängig von dieser Ländereinstellung das Datacenter, zu dem Ihre Backup geschickt werden. Stellen Sie sicher, dass Sie das Land wählen, in dem sich alle oder die Mehrheit aller Maschinen befinden, deren Backups Sie zum bzw. in den Cloud Storage speichern wollen. Ansonsten müssen die Daten über einen unnötig langen Weg verschickt werden. Sie können das Datacenter später nicht mehr ändern, auch dann nicht, wenn Sie das Land in Ihrem Profil ändern. Gehen Sie, um Zugriff auf Ihr Profil zu erhalten, zur Acronis-Website, wählen Sie dort den Bereich* ***Mein Konto****, melden Sie sich an – und klicken Sie anschließend auf* ***Persönliches Profil****.*

13.4.1 Abonnements in Acronis Backup aktivieren

So aktivieren Sie ein Abonnement

1. Starten Sie Acronis Backup.
2. Klicken Sie im Menü **Aktionen** auf **Cloud Backup-Abonnement aktivieren**
3. Spezifizieren Sie Benutzername und Kennwort zur Anmeldung am Cloud Storage.
4. Wählen Sie das Abonnement, welches Sie für die Maschine aktivieren wollen.
5. Klicken Sie auf **Jetzt aktivieren**.

13.4.2 Aktiviertes Abonnement erneut zuweisen

Manchmal möchten Sie vielleicht ein bereits aktiviertes Abonnement anstelle eines verfügbaren Abonnements verwenden. Typische Beispiele wären folgende:

- Sie benötigen bei einer der Maschinen keine Backups mehr und möchten das Abonnement dieser Maschine für ein andere verwenden.
- Sie haben auf einer Maschine Acronis Backup erneut installiert und möchten deren Cloud Backups fortsetzen.
- Sie haben die Maschine auf einer fabrikneuen Hardware wiederhergestellt (oder in einem Zustand, in dem noch kein Abonnement aktiviert war) und möchten deren Cloud Backups fortsetzen.

Wenn Sie ein Abonnement neu zuweisen, beginnt der Abonnementzeitraum nicht von Neuem.

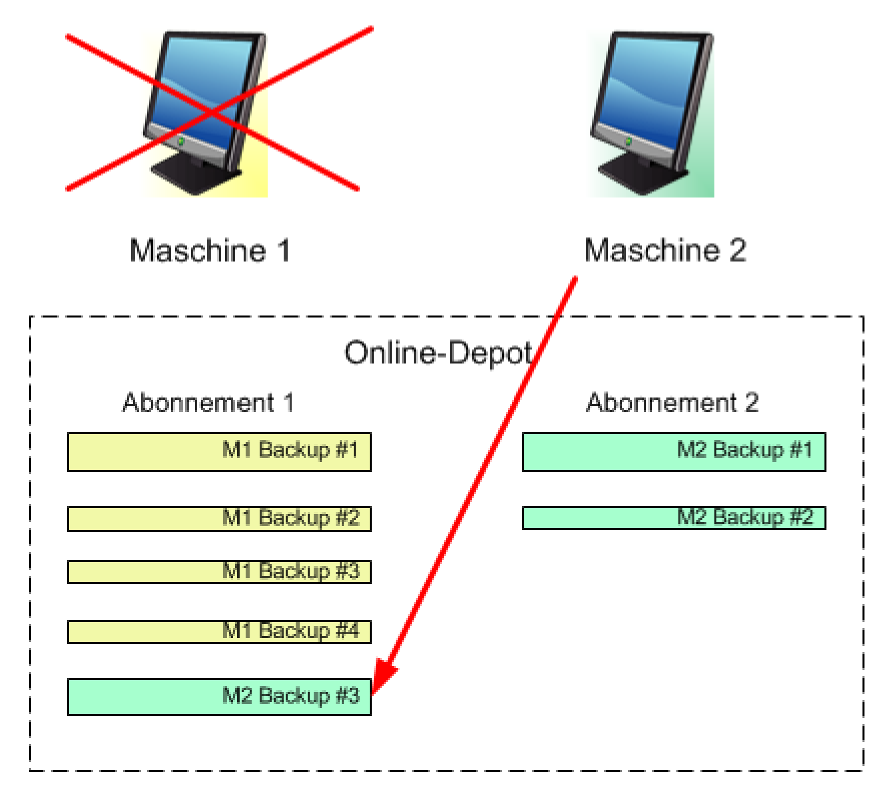
So weisen Sie einer Maschine ein aktiviertes Abonnement zu

1. Gehen Sie auf der Maschine, der Sie ein aktiviertes Abonnement zuweisen möchten, in das Fenster zum Aktivieren des Abonnements.
2. Klicken Sie auf **Ein bereits verwendetes Abonnement neu zuweisen**.
3. Wählen Sie die Maschine, deren Abonnement Sie der aktuellen Maschine neu zuweisen wollen.
4. Klicken Sie auf **Jetzt neu zuweisen**.

Beispiel

Das untere Diagramm verdeutlicht, was passiert, wenn Sie ein Abonnement einer anderen Maschine neu zuweisen. Angenommen, Maschine 1 hat vier Backups in Abonnement 1. Maschine 2 hat zwei Backups in Abonnement 2. Zu diesem Zeitpunkt weisen Sie das Abonnement 1 auf der Maschine 2 neu zu. Maschine 2 erstellt ihr drittes Backup unter Abonnement 1.

In Abhängigkeit von Ihren Einstellungen wird dieses Backup entweder vollständig oder inkrementell. Seine Größe ist aber vermutlich nicht geringer als die Größe eines Voll-Backups. Es ist daher nicht sinnvoll, ein Abonnement einer Maschine neu zuzuweisen, deren erstes Backup als Initial Seeding durchgeführt wurde. Sie müssen dann entweder das Initial Seeding erneut ausführen (was eine neue Lizenz erfordert) oder das ziemlich große Backup über das Internet übertragen.



Alle früher erstellten Backups verbleiben intakt. Sie können diese bei Bedarf auch manuell löschen. Beachten Sie aber, dass Backups von einem Abonnement nur durch die Maschine gelöscht werden können, der das Abonnement zugewiesen wurde. Sie haben beispielsweise folgende Optionen.

Vor erneuter Zuweisung

Löschen Sie Backups vom Abonnement 1 unter Verwendung von Maschine 1 (sofern verfügbar und angeschaltet). Löschen Sie Backups von Abonnement 2 unter Verwendung von Maschine 2.

Nach erneuter Zuweisung

Löschen Sie Backups von Abonnement 1 unter Verwendung von Maschine 2. Sie können Backups von Abonnement 2 nicht löschen, solange Sie dieses Abonnement keiner anderen Maschine zuweisen.

13.5 Proxy-Einstellungen konfigurieren

Wenn sich die Maschine zum Internet über einen Proxy-Server verbindet, müssen Sie Acronis Backup zu dessen Verwendung konfigurieren.

1. Starten Sie Acronis Backup.

2. Klicken Sie im Menü **Optionen** auf **Maschinen-Optionen**.
3. Klicken Sie auf **Cloud Backup Proxy**.
4. Tragen Sie die Einstellungen für den Proxy-Server ein. Konsultieren Sie die kontextabhängige Hilfe, um detaillierte Informationen (S. 270) zu den Einstellungen zu erhalten.

13.6 Dateien aus dem Cloud Storage mit einem Webbrowser abrufen

Sie können durch Verwendung eines Webbrowsers den Acronis Cloud Storage durchsuchen, den Inhalt von dateibasierten Archiven einsehen sowie ausgewählte Dateien und Ordner herunterladen.

Folgende Browser unterstützen diese Aktionen:

- Internet Explorer 7 oder später
- Mozilla Firefox 3.5 oder später
- Google Chrome 10 oder später
- Safari 5.0.5 oder später

So rufen Sie Dateien vom bzw. aus dem Cloud Storage ab:

1. Rufen Sie die Webseite zur Kontenverwaltung (S. 283) auf und klicken Sie auf den Befehl **Dateien aus der Acronis Cloud wiederherstellen**. Ihnen wird die Liste der Maschinen angezeigt, die mit dem spezifizierten Konto gesichert wurden. Die Liste der Maschinen, die ein Volume für mehrere Systeme gemeinsam nutzen, erscheint, wenn Sie dieses Abonnement wählen.
2. Klicken Sie auf den Namen der Maschine, deren Daten Sie abrufen wollen. Die Software zeigt Ihnen die Laufwerk- und Datei-Archive an, die die Daten dieser Maschine enthalten.

   Hinweis für Benutzer des Initial Seeding (S. 57)-Dienstes. Ein 'Initial Seeding'-Backup wird von Ihrem (eingesendeten) Festplattenlaufwerk in die Acronis Cloud Storage hochgeladen. Das Backup ist sichtbar, seine Daten sind jedoch hier nicht abrufbar.
3. Klicken Sie auf das gewünschte Datei-Archiv. Geben Sie auf Nachfrage das Archivkennwort ein. Die Software zeigt Ihnen alle jemals in dieses Archiv gesicherten Dateien und Ordner an.
4. Wechseln Sie bei Bedarf zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Details: Der Suchbegriff kann auch die Platzhalterzeichen (Wildcards) * und ? enthalten.
5. Wählen Sie eine der nachfolgenden Varianten:
   - Um von einer bestimmten Datei oder einem Ordner die jüngste Version zu erhalten, müssen Sie nur auf den entsprechenden Namen klicken.
   - Um von mehreren Dateien und Ordnern die jüngsten Versionen zu erhalten, aktivieren Sie die links danebenliegenden Kontrollkästchen und klicken Sie dann auf die Schaltfläche **Download**.
   - Um von einer bestimmten Datei eine frühere Version zu erhalten, klicken Sie auf das rechts danebenliegende Icon (⚙) und wählen Sie dann den Befehl **Versionen anzeigen**. Daraufhin öffnet sich ein Fenster mit einer Versionsliste. Wählen Sie in diesem Fenster die gewünschte Version per Datum und Uhrzeit aus und klicken Sie dann auf den Befehl **Download**.
   - [Bei Verwendung der Suche nicht verfügbar] Um frühere Versionen von mehreren Dateien und Ordnern abzurufen, wählen Sie den gewünschten Zeitpunkt aus der Liste **Versionen**. Aktivieren Sie die Kontrollkästchen links neben den Dateien bzw. Ordnern und klicken Sie dann auf die Schaltfläche **Download**.

     Details: Sie erhalten diejenigen Datei- bzw. Ordner-Versionen, die vor und möglichst nah zu dem gewählten Zeitpunkt per Backup gesichert wurden.

6. Klicken Sie auf **Speichern**, um die ausgewählten Dateien herunterzuladen.

   Details: Falls Sie eine einzelne Datei ausgewählt haben, wird diese wie vorliegend heruntergeladen. Ansonsten werden die gewählten Daten in eine .zip-Datei archiviert (mit dem vorgegebenen Namen 'AcronisArchive.zip').
7. Wählen Sie den Ort, wo die Daten abgelegt werden sollen und klicken Sie auf **Speichern**.

13.7 Beschränkungen des Cloud Storages

Abweichend von anderen, ebenfalls in Acronis Backup verfügbaren Storages hat der Cloud Storage folgende Einschränkungen.

Aktionen

Folgende Aktionen sind nicht möglich.

Backup-Aktionen:

- Backup mit einem bootfähigen Medium
- Backup mit dem Agenten für Exchange
- Erstellen differentieller Backups
- Verwendung des Backup-Schemas **Benutzerdefiniert**
- Vereinfachte Benennung von Backup-Dateien
- Simultanes, Host-basiertes Backup von mehreren virtuellen Maschinen
- Regelmäßige Konvertierung von Backups zu einer virtuellen Maschine einrichten

'**Aktionen mit Backups**':

- Ein Backup validieren*
- Backup exportieren
- Backup mounten
- Backups *aus* dem Cloud Storage replizieren oder verschieben
- Ein inkrementelles Backup zu einem vollständigen konvertieren

Aktionen mit Archiven (ein Archiv ist eine Zusammenstellung von Backups):

- Ein Archiv validieren
- Ein Archiv exportieren

Diese Einschränkungen gelten auch für Backups mit Initial Seeding bzw. Wiederherstellungen mit Large Scale Recovery.

* Ein 'Initial Seeding'-Backup wird direkt nach seiner Erstellung automatisch validiert.

Backup- und Recovery-Optionen

Einige Backup- und Recovery-Optionen werden bei Cloud Backups nicht unterstützt. Beispielsweise **Backup-Aufteilung** (S. 93).

Durch Verwendung der Option '**Backup-Performance –> Netzwerkverbindungsgeschwindigkeit**' können Sie die Übertragungsrate in Kilobyte pro Sekunde (aber nicht in Prozent) variieren.

13.8 Terminologiereferenz

Nachfolgend finden Sie einige Begriffe in Bezug auf Acronis Cloud Backup.

Ein Abonnement aktivieren

Ermöglicht der Maschine, den Cloud Storage in Übereinstimmung mit dem Abonnement zu verwenden.

Aktiviertes Abonnement

Ein Abonnement, das aktuell von einer Maschine verwendet wird.

Ein Abonnement einer Maschine zuweisen

Reservieren Sie ein Abonnement für eine bestimmte Maschine, um dessen aktuelles Abonnement zu erneuern.

Zugewiesenes Abonnement

Ein Abonnement, welches einer Maschine zugewiesen wurde.

Verfügbares Abonnement

Ein Abonnement, welches noch keiner Maschine zugewiesen wurde.

Extra-Service

Ein Dienst, den Sie zusätzlich zu den Cloud Backup-Abonnements verwenden können.

Die Storage-Quota vergrößern

Ersetzen Sie ein Abonnement durch ein anderes, das über eine größere Storage-Quota verfügt. Der verbleibende Abonnementzeitraum wird im Verhältnis zur vergrößerten Kapazität herabgesetzt.

Initial Seeding

Initial Seeding ist ein Extra-Service, bei dem Sie das anfängliche Voll-Backup lokal ausführen und dieses dann per Festplatte (oder mit einem vergleichbaren Laufwerk) an Acronis senden. Acronis lädt das Backup dann zum bzw. in den Cloud Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118 .

Large Scale Recovery

Large Scale Recovery ist ein Extra-Service, mit dem Sie eine Kopie der Backups abrufen können, welche sich im Cloud Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Der 'Large Scale Recovery'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118 .

Lizenz

Nicht zu verwechseln mit Produktlizenzen von Acronis Backup.

Erlaubnis für eine Maschine, einen Extra-Service von Acronis Cloud Backup zu verwenden.

Sie können 'Initial Seeding'-Lizenzen bzw. 'Large Scale Recovery'-Lizenzen erwerben.

Ein Abonnement neu zuweisen

Ein bereits aktiviertes Abonnement einer anderen Maschine zuweisen.

Registrierungscode

Zeichenkette zur Registrierung eines Abonnements oder einer Lizenz, die bei einem Acronis-Partner erworben wurde.

Wenn Sie ein solches Abonnement oder eine solche Lizenz erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jede von diesen. Danach tragen Sie diese Registrierungscodes auf der Webseite zur Kontoverwaltung ein – worauf diese Abonnements und Lizenzen zur Benutzung verfügbar werden.

Ein Abonnement erneuern

Weisen Sie ein Abonnement des gleichen Typs zu – und mit der gleichen oder einer größeren Storage Quota, als die des derzeitigen, aktivieren Abonnements.

Dieses Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Storage-Quota

Die Menge an Speicherplatz auf dem Online Storage, die auf Basis des Abonnements belegt werden kann.

Abonnement

Erlaubnis für eine oder mehrere Maschinen, eine bestimmte Menge an Speicherplatz für eine bestimmte Zeitdauer im Cloud Storage zu verwenden.

Abonnementzeitraum

Zeitraum, in dem ein Abonnement aktiviert bleibt. Sie können die Maschine während dieses Zeitraums sichern und wiederherstellen. Eine Wiederherstellung ist auch noch für weitere 30 Tage nach Ablauf des Zeitraums möglich.

Eine Abonnement-Zuweisung aufheben

Macht ein bereits zugewiesenes Abonnement wieder verfügbar.

Sie können die Zuweisung eines Abonnements aufheben, so lange es nicht aktiviert wurde.

14 Glossar

A

Acronis Active Restore

Geschützte Technologie von Acronis, die ein System sofort verfügbar macht, nachdem die Wiederherstellung des Systems angefangen hat. Das System bootet aus dem Backup (S. 299) und die Maschine wird betriebsbereit, um notwendige Dienste zur Verfügung zu stellen. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt. Beschränkungen:

- das Backup muss sich auf einem lokalen Laufwerk befinden (irgendeinem Gerät, das durch das BIOS verfügbar gemacht wird mit Ausnahmen des Bootens über das Netzwerk)
- Linux-Images werden nicht unterstützt
- GPT-Laufwerke und der UEFI-Boot-Modus werden nicht unterstützt.

Acronis Plug-in für WinPE

Modifikation von Acronis Backup Agent für Windows, die in einer Preinstallation Environment ausgeführt werden kann. Das Plugin kann mit Hilfe von Bootable Media Builder zu einem Image für WinPE (S. 306) hinzugefügt werden. Die resultierenden bootfähigen Medien (S. 296) können benutzt werden, jede PC-kompatible Maschine zu starten – und, mit gewissen Einschränkungen, die meisten direkten Verwaltungsaufgaben (S. 298) ohne Hilfe des Betriebssystems auszuführen. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 301) konfiguriert und gesteuert werden.

Acronis Secure Zone

Ein geschütztes Volume zum Speichern von Backup-Archiven (S. 294) innerhalb einer verwalteten Maschine (S. 305). Vorteile:

- ermöglicht die Wiederherstellung eines Laufwerks auf dasselbe Laufwerk, auf der auch die Laufwerk-Backups hinterlegt sind
- bietet eine kosteneffektive und handliche Methode zum Schutz vor Softwarefehlern, Virusangriffen, Bedienerfehlern
- beseitigt die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders für mobile Benutzer nützlich.
- kann als primärer Speicherort dienen, von wo aus Backups dann weiter repliziert werden.

Einschränkung: die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk (S. 299) organisiert werden.

Die Acronis Secure Zone wird als persönliches Depot (S. 303) betrachtet.

Acronis Startup Recovery Manager (ASRM)

Eine Modifikation des bootfähigen Agenten (S. 296), auf dem Systemlaufwerk liegend und konfiguriert, um beim Booten zu starten, wenn die Taste F11 gedrückt wird. Acronis Startup Recovery

Manager bietet eine Alternative zu Rettungsmedien oder einer Netzwerkverbindung, um ein bootfähiges Rettungswerkzeug zu starten.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, bootet der Benutzer die Maschine neu, drückt die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ erscheint, und stellt dann die Daten auf die gleiche Weise wie mit den gewöhnlichen bootfähigen Medien wieder her.

Einschränkungen: Erfordert die Reaktivierung von Boot-Loadern außer Windows-Loadern und GRUB.

Acronis Universal Restore

Eine proprietäre Acronis-Technologie, um Windows oder Linux auf abweichender Hardware oder einer virtuellen Maschine bootfähig zu machen. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

Universal Restore ist nicht verfügbar:

- wenn das wiederherzustellende Image in der Acronis Secure Zone (S. 293) liegt oder
- wenn Acronis Active Restore (S. 293) verwendet wird,

weil alle diese Funktionen in erster Linie zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Agent (Acronis Backup Agent)

Anwendung, die das Backup und die Wiederherstellung von Daten und andere Verwaltungsaufgaben auf der Maschine (S. 302) ermöglicht, wie z.B. die Task-Verwaltung und Aktionen mit Festplatten.

Die Art Daten, die gesichert werden können, hängt vom Typ des Agenten ab. Acronis Backup enthält die Agenten für das Backup von Festplatten und Dateien und die Agenten für das Backup virtueller Maschinen, die auf Virtualisierungs-Servern bereitgestellt werden.

Aktivität

Eine von Acronis Backup durchgeführte Aktion, die dem Erreichen eines bestimmten, vom Benutzer gesteckten Ziels dient. Beispiele: Backup, Recovery, Export eines Backups, Katalogisierung eines Depots. Eine Aktivität kann durch einen Benutzer oder die Software selbst initiiert werden. Die Ausführung eines Tasks (S. 304) verursacht immer eine oder mehrere Aktivitäten.

Archiv

Siehe Backup-Archiv (S. 295).

Aufbewahrungsregeln

Der Teil eines Backup-Plans (S. 295), der spezifiziert, wann und wie von diesem Plan erstellte Backups (S. 294) gelöscht oder verschoben werden sollen.

B

Backup

Ein Backup ist das Ergebnis einer einzelnen Backup-Aktion. Physikalisch gesehen handelt es sich um eine Datei oder Bandaufzeichnung, die eine Kopie der gesicherten Daten zu einem spezifischen Zeitpunkt enthält. Backup-Dateien, die von Acronis Backup erstellt wurden, haben die Dateierweiterung tib. TIB-Dateien, die das Ergebnis eines Backup-Exports (S. 300) oder Konsolidierung (S. 301) sind, werden ebenfalls als Backups bezeichnet.

Backup (Aktion)

Aktion, die eine Kopie der Daten erstellt, die auf der Festplatte einer Maschine (S. 302) existieren, um diese wiederherzustellen oder in den Zustand zu einem festgelegten Tag bzw. Zeitpunkt zurückzusetzen.

Backup-Archiv (Archiv)

Satz von Backups (S. 294), die mit einem Backup-Plan (S. 295) erstellt und verwaltet werden. Ein Archiv kann mehrere Voll-Backups (S. 306) enthalten, aber auch inkrementelle (S. 301) und differentielle Backups (S. 298). Backups, die zum gleichen Archiv gehören, werden immer am gleichen Ort gespeichert. Falls ein Backup-Plan eine Replikation (S. 303) oder Verschiebung von Backups zu weiteren Speicherorten beinhaltet, dann bilden die Backups an jedem dieser Speicherorte ein separates Archiv.

Backup-Optionen

Konfiguration der Parameter für eine Backup-Aktion, wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt wird, oder die Datenkomprimierungsrate. Backup-Optionen sind Bestandteil eines Backup-Plans (S. 295).

Backup-Plan (Plan)

Ein Satz von Regeln, der spezifiziert, wie gegebene Daten auf einer bestimmten Maschine geschützt bzw. gesichert werden sollen. Ein Backup-Plan spezifiziert:

- welche Daten gesichert werden sollen
- den Namen und Speicherort des Backup-Archivs (S. 295)
- das Backup-Schema (S. 296). Das schließt eine Backup-Planung und [optional] Aufbewahrungsregeln (S. 294) mit ein
- [optional] zusätzliche Aktionen, die mit den Backups durchgeführt werden sollen (Replikation (S. 303), Validierung (S. 305), Konvertierung zu einer virtuellen Maschine)
- die Backup-Optionen (S. 295).

Ein Backup-Plan kann beispielsweise folgende Informationen enthalten:

- führe ein Backup von Volume C: aus **(das sind die Daten, die der Plan schützt)**
- benenne das Archiv 'MeinSystemVolume' und speichere es in '\\server\backups' **(Name und Speicherort des Backup-Archivs)**
- führe ein monatliches Voll-Backup am letzten Tag des Monats um 10:00 Uhr aus und ein inkrementelles Backup an Sonntagen um 22:00 Uhr. Lösche Backups, die älter sind als 3 Monate **(das ist das Backup-Schema)**

- validiere das letzte Backup unmittelbar nach seiner Erstellung **(das ist die Validierungsregel)**
- schütze das Archiv mit einem Kennwort **(das ist eine Option)**.

Physikalisch ist ein Backup-Plan ein Zusammenstellung von Tasks (S. 304), die auf einer verwalteten Maschine (S. 305) ausgeführt werden.

Ein Backup-Plan kann direkt auf der Maschine erstellt werden, von einer anderen Maschine importiert werden (lokaler Plan) oder vom Management Server auf die Maschine verbreitet werden (zentraler Plan (S. 307)).

Backup-Schema

Teil eines Backup-Plans (S. 295), der den Zeitplan für das Backup und [optional] die Aufbewahrungsregeln und den Zeitplan für die Bereinigung (S. 296) mit einschließt. Beispielsweise führe monatlich ein Voll-Backup (S. 306) am letzten Tag des Monats um 10:00 Uhr aus – und ein inkrementelles Backup (S. 301) an Sonntagen um 22:00 Uhr. Lösche Backups, die älter sind als 3 Monate. Prüfe auf solche Backups jedes Mal, wenn ein Backup abgeschlossen wurde.

Acronis Backup bietet die Möglichkeit, bekannte optimierte Backup-Schemata wie zum Beispiel GVS und Türme von Hanoi zu verwenden, benutzerdefinierte Backup-Schemata zu erstellen oder alle Daten auf einmal zu sichern.

Bereinigung

Löschen von Backups (S. 294) aus einem Backup-Archiv (S. 295) oder Verschieben zu einem anderen Speicherort, um veraltete Backups zu entfernen oder um zu verhindern, dass das Archiv die gewünschte Größe zu überschreitet.

Eine Bereinigung besteht in derAnwendung von Aufbewahrungsregeln (S. 294) auf ein Archiv. Die Aufbewahrungsregeln werden durch den Backup-Plan (S. 295) eingerichtet, der das Archiv produziert. Eine Bereinigung kann (muss aber nicht) dazu führen, dass Backups gelöscht oder verschoben werden, je nachdem, ob die Aufbewahrungsregeln verletzt wurden oder nicht.

Bootable Agent

Bootfähiges Wiederherstellungswerkzeug, das die meisten Funktionen von Acronis Backup Agent (S. 294) enthält. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine (S. 302) kann entweder mit Hilfe bootfähiger Medien (S. 296) oder über den Acronis PXE Server in den bootfähigen Agenten gestartet werden. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 301) konfiguriert und gesteuert werden.

Bootfähiges Medium

Physikalisches Medium (CD, DVD, USB-Sticks oder andere von einer Maschine (S. 302) als Boot-Gerät unterstützt Medien), die den bootfähigen Agenten (S. 296) oder die Windows Preinstallation Environment (WinPE) (S. 306) mit dem Acronis Plug-in für WinPE (S. 293) enthalten. Eine Maschine kann außerdem mit einer der genannten Umgebungen gestartet werden, wenn die Möglichkeit genutzt wird, per Acronis PXE-Server oder Windows Deployment Service (WDS) über das Netzwerk zu booten. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiges Medium angesehen werden.

Bootfähige Medien werden am häufigsten verwendet, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet

- auf Daten zuzugreifen und zu sichern, die in einem beschädigten System überlebt haben
- ein Betriebssystem auf fabrikneue Computer zu verteilen
- Basis-Volumes oder dynamische Volumes (S. 300) auf fabrikneuen Festplatten (bzw. ähnlichen Laufwerken) einzurichten
- Laufwerke mit nicht unterstütztem Dateisystem per Sektor-für-Sektor-Backup zu sichern
- Daten 'offline' zu sichern, die wegen einer Zugangsbeschränkung, einer Sperrung durch laufende Anwendungen oder wegen anderer Gründe nicht 'online' gesichert werden können.



Datenkatalog

Der Datenkatalog ermöglicht Benutzern, die benötigten Versionen bestimmter Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen. Benutzer können auf einer verwalteten Maschine (S. 305) Daten in jedem Depot (S. 298), auf das von dieser Maschine Zugriff besteht, einsehen und suchen. Der auf dem Management Server (S. 302) verfügbare zentrale Katalog enthält alle auf seinen Storage Nodes (S. 304) gespeicherten Daten.

Physikalisch wird der Datenkatalog in Katalogdateien gespeichert. Jedes Depot verwendet seinen eigenen Satz an Katalogdateien, die normalerweise direkt im Depot vorliegen. Sollte dies nicht möglich sein, wie etwa bei Band-Storages, dann werden die Katalogdateien in einem lokalen Ordner der verwalteten Maschine oder des Storage Nodes gespeichert. Ein Storage Node speichert zudem die Katalogdateien seiner Remote-Depots auch lokal, um so einen schnelleren Zugriff zu erreichen.

Datenträgergruppe

Anzahl dynamischer Laufwerke (S. 299), die ihre Konfigurationendaten in ihren LDM-Datenbanken speichern und deshalb als ein Ganzes verwaltet werden können. Normalerweise sind alle dynamischen Datenträger, die innerhalb der gleichen Maschine (S. 302) erstellt wurden, Mitglieder der gleichen Datenträgergruppe.

Sobald das erste dynamische Datenträger vom LDM oder einem anderen Festplattenverwaltungswerkzeug erstellt wird, kann der Name der Datenträgergruppe im Registry-Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name gefunden werden.

Das nächste erstellte oder importierte Datenträger wird zur gleichen Datenträgergruppe hinzugefügt. Die Gruppe existiert, so lange wenigstens eine ihrer Mitglieder existiert. Nachdem der letzte dynamische Datenträger abgeschaltet oder in einen Basisdatenträger konvertiert wurde, ist die Gruppe stillgelegt, obwohl der Name im oben genannten Registry-Key erhalten bleibt. Falls erneut ein dynamischer Datenträger erstellt oder wieder angeschlossen wird, wird eine Datenträgergruppe mit einem inkrementellen Namen erstellt.

Wenn eine Datenträgergruppe zu einer anderen Maschine verschoben wird, wird sie als „fremd“ betrachtet und kann nicht benutzt werden, bis sie in eine existierende Datenträgergruppe importiert wird. Der Import aktualisiert die Konfigurationsdaten auf den lokalen und den 'fremden' Datenträgern, damit sie eine Einheit bilden. Eine 'fremde' Gruppe wird importiert, wie sie ist (wird den ursprünglichen Namen haben), wenn keine Datenträgergruppe auf der Maschine existiert.

Weitere Informationen über Datenträgergruppen finden Sie auf den Microsoft-Webseiten:

222189 Beschreibung der Datenträgergruppen in der Windows Datenträgerverwaltung http://support.microsoft.com/kb/222189/de

Deduplizierendes Depot

Verwaltetes Depot (S. 305) mit aktivierter Deduplizierung (S. 298).

Deduplizierung

Methode, um identische Informationen in verschiedenen Kopien nur einmalig zu speichern.

Acronis Backup kann die Deduplizierungstechnologie auf Backup-Archive (S. 295) anwenden, die auf Storage Nodes (S. 304) gespeichert sind. Das reduziert den für Archive benötigten Speicherplatz, den Backup-Datentransfer sowie die Netzwerkauslastung während der Backup-Erstellung.

Depot

Ort für die Ablage von Backup-Archiven (S. 295). Ein Depot kann auf einem lokalen Laufwerk, auf einem Netzlaufwerk oder auf einem entfernbaren Medium wie einem USB-Laufwerk organisiert werden. Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung (S. 296) begrenzen, aber die Gesamtgröße der Archive in einem Depot wird nur durch die Größe des Speichers selbst begrenzt.

Desaster-Recovery-Plan (DRP)

Ein Dokument, die eine Liste von per Backup gesicherten Datenelementen sowie genaue Anweisungen enthält, wie diese Elemente aus dem Backup wiederhergestellt werden sollen.

Wird die entsprechende Backup-Option (S. 295) aktiviert, dann wird ein DRP erstellt, sobald das erste Backup erfolgreich vom Backup-Plan durchgeführt wurde – und ebenso, wenn sich die Liste der Datenelemente oder die DRP-Parameter ändern sollten. Dein DRP kann an die spezifizierten E-Mail-Adressen gesendet oder als Datei in einem lokalen Ordner oder Netzwerkordner gespeichert werden.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 306). Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen.

Direkte Verwaltung

Eine Aktion, die auf einer verwalteten Maschine (S. 305) unter Verwendung einer direkten Verbindung zwischen Konsole (S. 301) und Agent (S. 294) ausgeführt wird (im Gegensatz zur zentraler Verwaltung (S. 306), bei der Aktionen auf dem Management Server (S. 302) konfiguriert und dann durch den Server auf die verwalteten Maschinen verbreitet werden).

Die direkten Verwaltungsaktionen umfassen:

- Erstellung und Verwaltung lokaler Backup-Pläne (S. 302)
- Erstellung und Verwaltung lokaler Tasks (S. 302), wie z.B. Recovery-Tasks
- Erstellung und Verwaltung persönlicher Depots (S. 303) und der dort gespeicherten Archive
- Anzeige der Stadien, Fortschritte und Eigenschaften derjenigen zentralen Tasks (S. 307), die auf der Maschine vorkommen
- Anzeige und Verwaltung von Logs der Aktionen des Agenten

- Laufwerksverwaltungsaktionen wie das Klonen eines Laufwerks sowie das Erstellen und Konvertieren von Volumes.

Bei Verwendung von bootfähigen Medien (S. 296) erfolgt auch eine Art direkte Verwaltung.

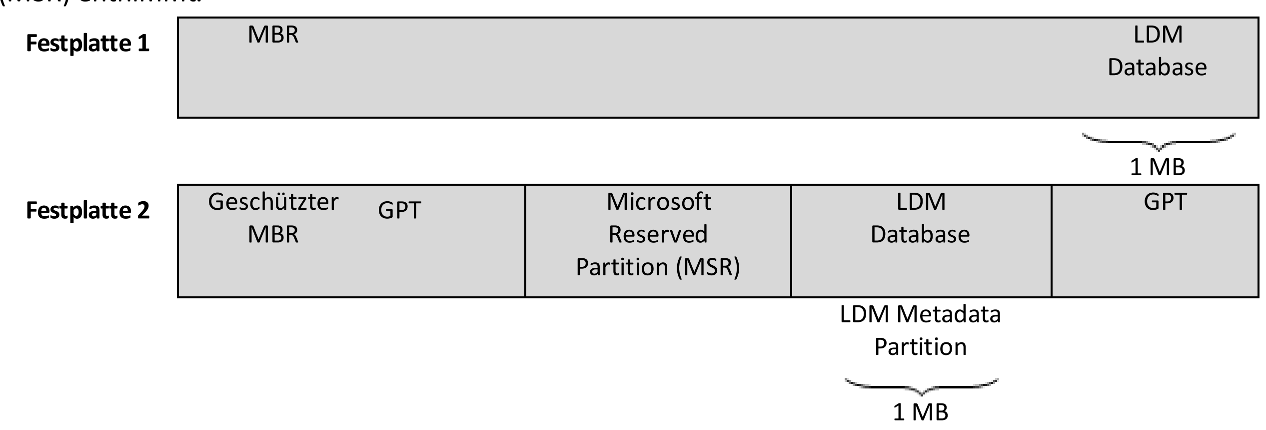
Disk-Backup (Image)

Backup (S. 294), das eine auf den Sektoren basierende Kopie einer Festplatte oder Partition in gepackter Form enthält. Normalerweise werden nur Sektoren kopiert, die Daten enthalten. Acronis Backup bietet aber eine Option, um Raw-Images zu erstellen, d.h. alle Sektoren zu kopieren, um z.B. das Imaging nicht unterstützter Dateisysteme zu ermöglichen.

Dynamische Festplatten

Laufwerk, das vom Logical Disk Manager (LDM) verwaltet wird, der in Windows seit Windows 2000 verfügbar ist. LDM unterstützt die flexible Zuweisung von Volumes auf einem Speichergerät für bessere Fehlertoleranz, bessere Leistung oder eine höhere Volume-Größe.

Ein dynamisches Laufwerk kann entweder das Partitionierungsschema 'Master Boot Record' (MBR) oder 'GUID-Partitionstabelle' (GPT) verwenden. Zusätzlich zu MBR oder GPT hat jedes dynamische Laufwerk eine versteckte Datenbank, wo der LDM die Konfiguration der dynamischen Volumes speichert. Jedes dynamische Laufwerk hält für eine bessere Speicherzuverlässigkeit die vollständigen Informationen über alle dynamischen Laufwerke bereit, die in der Datenträgergruppe existieren. Die Datenbank besetzt das letzte Megabyte einer MBR-Festplatte. Auf einer GPT-Festplatte erstellt Windows eine dedizierte LDM-Metadaten-Partition, die Platz von der Microsoft Reserved Partition (MSR) entnimmt.



Organisation dynamischer Festplatten auf Basis MBR (Festplatte 1) und GPT (Festplatte 2).

Weitere Informationen über dynamische Datenträger finden Sie im Artikel der Microsoft Knowledgebase:

Disk Management (Windows XP Professional Resource Kit) http://technet.microsoft.com/de-de/library/bb457110.aspx

816307 Empfohlene Verfahrensweisen für die Verwendung dynamischer Datenträger auf Windows Server 2003-Computern http://support.microsoft.com/kb/816307/de .

Dynamische Gruppe

Gruppe von Maschinen (S. 302), die automatisch vom Management Server (S. 302) gemäß der Kriterien für die Mitgliedschaft aufgefüllt wird, die vom Administrator angegeben werden. Acronis Backup bietet folgende Mitgliedschaftskriterien:

- Betriebssystem
- Active Directory-Organisationseinheit
- IP-Adressbereich
- In txt/csv-Datei aufgelistet.

Eine Maschine verbleibt in einer dynamischen Gruppe, solange die Maschine die Kriterien der Gruppe erfüllt. Der Administrator kann jedoch Ausschließungen spezifizieren und so gewisse Maschinen nicht in der dynamischen Gruppe enthalten sein lassen, auch wenn sie die Kriterien erfüllen.

Dynamisches Volume

Volume, das sich auf auf einem dynamischen Datenträger (S. 299) oder genauer auf einer Datenträgergruppe (S. 297) befindet. Dynamische Volumes können sich über mehrere Laufwerke erstrecken. Dynamische Datenträger sind gewöhnlich abhängig vom gewünschten Ziel gestaltet:

- um die Größe zu erweitern (übergreifendes Volume)
- um die Zugriffszeit zu verringern (Stripesetvolume)
- um die Fehlertoleranz durch redundante Informationen zu erreichen (gespiegelte und RAID-5-Volumes).

E

Exportieren

Eine Aktion, bei der eine Kopie bzw. unabhängige Teilkopie eines Archivs (S. 295) am von Ihnen angegebenen Speicherort erstellt wird. Ein Export kann ein einziges Archiv, ein einziges Backup (S. 294) oder eine Auswahl von Backups aus dem gleichen Archiv umfassen. Ein vollständiges Depot (S. 298) kann über die Befehlszeilenschnittstelle exportiert werden.



GVS (Großvater-Vater-Sohn)

Populäres Backup-Schema (S. 296), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 295) und der Anzahl von Wiederherstellungspunkten (S. 306) sorgen soll, die im Archiv enthalten sind. GVS ermöglicht ein Recovery mit täglicher Rasterung für die letzten Tage, wöchentlicher Rasterung für die letzten Wochen und monatlicher Rasterung für jede Zeit in der Vergangenheit.

Weitere Informationen finden Sie bei Backup-Schema GVS.

I

Image

Gleichbedeutend mit Disk-Backup (S. 299).

Indizierung

Eine Aktivität (S. 294), von einem Storage Node (S. 304) durchgeführt, nachdem ein Backup (S. 294) zu einem deduplizierenden Depot (S. 297) gespeichert wurde.

Der Storage Node führt während der Indizierung folgende Aktionen aus:

- Er verschiebt Datenblöcke von dem Backup zu einer speziellen Datei innerhalb des Depots. Diese Datei wird Deduplizierungsdatenspeicher genannt.
- In dem Backup werden die verschobenen Blöcke durch ihre 'Fingerabdrücke' (Hash-Werte) ersetzt.
- Er speichert die Hash-Werte und die Links, die zum Zusammensetzen der deduplizierten Daten notwendig sind, in der Deduplizierungsdatenbank.

Eine Indizierung kann man sich als 'Deduplizierung am Ziel' vorstellen – im Gegensatz zur 'Deduplizierung an der Quelle', welche der Agent (S. 294) während einer Backup-Aktion ausführt. Ein Benutzer kann die Indizierung anhalten und wieder neu aufnehmen.

Inkrementelles Backup

Ein Backup (S. 294), das Datenänderungen in Bezug zum letzten Backup speichert. Sie müssen auf andere Backups des gleichen Archivs (S. 295) zugreifen können, um Daten aus einem inkrementellen Backup wiederherstellen zu können.



Katalogisierung

Beim Katalogisieren eines Backups (S. 294) werden dessen Inhalte zum Datenkatalog (S. 297) hinzugefügt. Backups werden automatisch katalogisiert, sobald Sie erstellt wurden. Backups, die auf einem Storage Node (S. 304) gespeichert sind, werden automatisch durch den Knoten katalogisiert. Backups, die irgendwo anders gespeichert sind, werden durch den Agenten (S. 294) katalogisiert. Der Benutzer kann in den Backup-Optionen (S. 295) zwischen vollständiger und schneller Katalogisierung wählen. Die vollständige Katalogisierung kann außerdem auch manuell gestartet werden.

Konsole (Acronis Backup Management Console)

Werkzeug für den Remote- oder lokalen Zugriff auf Acronis Agenten (S. 294) und den Acronis Backup Management Server (S. 302).

Wenn die Konsole mit dem Management Server verbunden ist, kann der Administrator zentrale Backup-Pläne (S. 307) einrichten sowie auf andere Funktionen des Management-Servers zugreifen, d.h. er arbeitet mit zentraler Verwaltung (S. 306). Wenn der Administrator eine direkte Verbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 298).

Konsolidierung

Kombinieren zweier oder weiterer subsequenter Backups (S. 294), die zum gleichen Archiv (S. 295) gehören, in ein Backup.

Konsolidierung könnte beim Löschen von Backups gebraucht werden, entweder manuell oder während der Bereinigung (S. 296). Zum Beispiel könnten die Aufbewahrungsregeln erfordern, ein abgelaufenes Voll-Backup (S. 306) zu löschen, aber die nächste inkrementelle Sicherung (S. 301) zu erhalten. Die Backups werden in ein einzelnes Voll-Backup kombiniert und mit dem Datum des

inkrementellen Backups versehen. Da die Konsolidierung viel Zeit und Systemressourcen beansprucht, bieten die Aufbewahrungsregeln eine Option, Backups mit Abhängigkeiten nicht zu löschen. Im Beispiel wird das Voll-Backup erhalten, bis auch das inkrementelle Backup veraltet ist. Dann werden beide Backups gelöscht.

L

Logisches Volume

Dieser Begriff hat zwei Bedeutungen, abhängig vom Kontext.

- Ein Volume, dessen Information in einer erweiterten Partitionstabelle gespeichert wird. (Im Gegensatz zu einem primären Volume, dessen Information im Master Boot Record gespeichert wird).
- Ein Volume, das unter Verwendung des Logical Volume Managers (LVM) des Linux-Kernels erstellt wurde. LVM gibt einem Administrator die Flexibilität, große Speicherplatzmengen je nach Bedarf zu verteilen und ohne Unterbrechung der Systemnutzung neue physikalische Laufwerke hinzuzufügen oder alte herauszunehmen. Der Acronis Backup Agent (S. 294) für Linux kann auf logische Volumes zugreifen, sie sichern und wiederherstellen, wenn er unter Linux mit 2.6-Kernel oder von einem Linux-basierten bootfähigen Medium (S. 296) ausgeführt wird.

Lokaler Backup-Plan

Backup-Plan (S. 295), erstellt auf einer verwalteten Maschine (S. 305) durch direkte Verwaltung (S. 298).

Lokaler Task

Ein auf einer verwalteten Maschine (S. 305) durch direkte Verwaltung (S. 298) erstellter Task (S. 304).

M

Management Server (Acronis Backup Management Server)

Zentraler Server zur Datensicherung innerhalb des Unternehmensnetzes. Acronis Backup Management Server versorgt den Administrator mit:

- einen zentralen Zugriffspunkt auf die Acronis Backup-Infrastruktur
- einen einfachen Weg zur Sicherung von Daten auf zahlreichen Maschinen (S. 302) – durch Verwendung von zentralen Backup-Plänen (S. 307) und Gruppierung
- unternehmensweitem Monitoring und Berichtsfunktionalität
- der Fähigkeit, zentrale Depots (S. 307) zur Speicherung der Backup-Archive (S. 295) des Unternehmens zu erstellen
- der Fähigkeit, Storage Nodes (S. 304) zu verwalten
- einen zentralen Katalog (S. 297) aller Daten, die auf Storages Nodes gespeichert sind.

Gibt es mehrere Management Server im Netzwerk, dann arbeiten diese unabhängig voneinander, verwalten verschiedene Maschinen und verwenden verschiedene zentrale Depots zur Speicherung von Archiven.

Maschine

Ein physikalischer oder virtueller Computer, der eindeutig anhand seiner Betriebssysteminstallation identifiziert wird. Maschinen mit mehreren Betriebssystemen (Multi-Boot-Systeme) werden auch als mehrfache Maschinen betrachtet.

Media Builder

Spezielles Werkzeug zum Erstellen bootfähiger Medien (S. 296).

N

Nicht verwaltetes Depot

Jedes Depot (S. 298), das kein verwaltetes Depot (S. 305) ist.

P

Persönliches Depot

Lokales oder im Netzwerk befindliches Depot (S. 298), das durch direkte Verwaltung (S. 298) erstellt wurde. Sobald ein persönliches Depot erstellt wurde, erscheint auf der verwalteten Maschine eine Verknüpfung zu diesem in der Liste **Depots**. Mehrere Maschinen können den gleichen physikalischen Speicherort benutzen, z.B. ein freigegebenes Netzlaufwerk oder ein persönliches Depot.

Plan

Siehe Backup-Plan (S. 295).

R

Registrierte Maschine

Maschine (S. 302), die durch einen Management Server (S. 302) verwaltet wird. Eine Maschine kann zur gleichen Zeit nur auf einem Management Server registriert sein. Eine registrierte Maschine entsteht durch ein Verfahren zur Registrierung (S. 303).

Registrierung

Verfahren, das eine verwaltete Maschine (S. 305) zu einem Management Server (S. 302) hinzufügt.

Die Registrierung stellt eine Vertrauensstellung zwischen dem Agenten (S. 294) auf der Maschine und dem Server her. Während der Registrierung ruft die Konsole das Client-Zertifikat des Management Servers ab und leitet es an den Agent weiter, der es später beim Herstellen der Verbindung zur Authentifizierung benutzt. Dies hilft, Versuche von Angreifern des Netzwerks zu verhindern, eine Verbindung unter Vortäuschung eines vertrauten Auftraggebers (des Management Servers) herzustellen.

Replikation

Eine Replikation entspricht dem Kopieren eines Backups (S. 294) zu einem anderen Speicherort. Das Backup wird standardmäßig direkt nach seiner Erstellung kopiert. Durch die Konfiguration einer Inaktivitätszeit erhält der Benutzer die Option, das Kopieren des Backups aufzuschieben.

Diese Funktion ersetzt und erweitert die Backup-Option 'Dual-Destination', wie sie in Acronis Backup & Recovery 10 verfügbar war.

S

Single-Pass-Backup

Ein Single-Pass-Backup (Einzeldurchlauf-Backup, auch als anwendungssensitives Backup bekannt) ist ein Laufwerk-Backup, welches Metadaten von VSS-kompatiblen Anwendungen enthält, die auf dem Laufwerk vorliegen. Diese Metadaten ermöglichen es, die per Backup gesicherten Anwendungsdaten zu durchsuchen und wiederherzustellen, ohne das komplette Laufwerk oder Volume wiederherstellen zu müssen.

Standardgruppe

Eine Gruppe von Maschinen, die permanent auf einem Management Server (S. 302) vorliegen.

Diese eingebauten Standardgruppen können nicht gelöscht, zu anderen Gruppen verschoben oder manuell modifiziert werden. Benutzerdefinierte Gruppen können nicht innerhalb von Standardgruppen erstellt werden. Es gibt keinen anderen Weg, eine Maschine aus der Standardgruppe zu entfernen, als diese vom Management Server zu entfernen.

Statische Gruppe

Maschinengruppe, die der Administrator eines Management Servers (S. 302) durch manuelles Hinzufügen von Maschinen zur betreffenden Gruppe auffüllt. Eine Maschine verbleibt in einer statischen Gruppe, bis der Administrator diese von der Gruppe oder vom Management Server entfernt.

Storage Node (Acronis Backup Storage Node)

Server, der zur optimierten Nutzung verschiedener Ressourcen gedacht ist, die zum Schutz von Unternehmensdaten erforderlich sind. Dieses Ziel wird durch die Organisation von verwalteten Depots (S. 305) erreicht. Dank eines Storage Nodes kann ein Administrator:

- einen einzelnen zentralen Katalog (S. 297) für alle in verwalteten Depots gespeicherte Daten verwenden
- verwaltete Maschinen (S. 305) von unnötiger CPU-Last befreien, indem Bereinigungen (S. 296), Validierungen (S. 305) und anderen Aktionen mit den Backup-Archiven (S. 295) durchgeführt werden, die sonst von den Agenten (S. 294) ausgeführt würden
- den von Archiven (S. 295) verursachten Backup-Datentransfer und belegten Speicherplatz durch Verwendung von Deduplizierung (S. 298) drastisch senken
- mit Hilfe verschlüsselter Depots (S. 305) den Zugriff auf Backup-Archive verhindern, auch wenn das Speichermedium gestohlen wird oder es zu unbefugtem Zugriff auf die Archive kommt.

T

Task

Ein Satz von Aktionen, der von Acronis Backup zu einem bestimmten Zeitpunkt oder auf ein Ereignis hin durchgeführt wird. Die Aktionen sind in einer nicht vom Benutzer lesbaren Service-Datei beschrieben. Zeitpunkt oder Ereignis (für die Planung) werden in einem geschützten Registry-Schlüssel (in Windows) oder im Dateisystem (in Linux) gespeichert.

Türme von Hanoi

Populäres Backup-Schema (S. 296), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 295) und der Anzahl von Wiederherstellungspunkten (S. 306) sorgen soll, die im Archiv enthalten sind. Im Gegensatz zum GVS (S. 300)-Schema, das lediglich drei Level für die Wiederherstellungsauflösung hat (täglich, wöchentlich und monatlich), ist es mit dem Schema „Türme von Hanoi" möglich, den zeitlichen Abstand zwischen Wiederherstellungspunkten bei steigendem Alter des Backups kontinuierlich zu reduzieren. Das ermöglicht eine sehr effiziente Verwendung des Backup-Speichers.

Weitere Informationen finden Sie unter Backup-Schema „Türme von Hanoi" (S. 54).



Validierung

Aktion, mit der die Möglichkeit einer Datenwiederherstellung aus einem Backup (S. 294) geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Laufwerk-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Beide Prozeduren sind ressourcenintensiv.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie das Betriebssystem gesichert haben, kann nur eine testweise Wiederherstellung unter Verwendung eines bootfähigen Mediums auf einem Ersatzlaufwerk eine zukünftige erfolgreiche Wiederherstellung garantieren.

Verschlüsseltes Archiv

Ein Backup-Archiv (S. 295), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Ist die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 295) definiert, dann wird jedes zum Archiv gehörende Backup vom Agenten (S. 294) noch vor dem Ablegen des Backups am Zielort verschlüsselt.

Verschlüsseltes Depot

Verwaltetes Depot (S. 305), bei dem ein Storage Node (S. 304) alles dorthin Geschriebene verschlüsselt bzw. alles von dort Gelesene transparent entschlüsselt, wobei ein für das Depot spezifischer Encryption Key benutzt wird, der auf dem Knoten gespeichert ist. Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf den Storage Node nicht entschlüsseln können. Verschlüsselte Archive (S. 305) werden über die Verschlüsselung des Agenten (S. 294) erstellt.

Verwaltete Maschine

Physikalische oder virtuelle Maschine (S. 302), auf der wenigstens ein Acronis Backup (S. 294) Agent installiert ist.

Verwaltetes Depot

Ein zentrales Depot (S. 307), welches von einem Storage Node (S. 304) verwaltet wird. Auf Archive (S. 295) in einem verwalteten Depot kann folgendermaßen zugegriffen werden:

bsp://knoten_adresse/depot_name/archiv_name/

Physikalisch können sich verwaltete Depots auf einem freigegebenen Netzlaufwerk, einem SAN, NAS, auf einer lokalen Festplatte des Storage Nodes oder einer Bandbibliothek befinden, die lokal an den Storage Node angeschlossen ist. Der Storage Node führt Bereinigungen (S. 296) und Validierungen (S. 305) für jedes im verwalteten Depot gespeicherte Archiv durch. Ein Administrator kann zusätzliche Aktionen spezifizieren, die der Storage Node durchführen soll, z.B. Deduplizierung (S. 298) oder Verschlüsselung.

Virtuelle Maschine

Auf dem Acronis Backup Management Server (S. 302) wird eine Maschine (S. 302) als 'virtuell' betrachtet, wenn sie per Backup vom Virtualisierungshost gesichert werden kann, ohne dass dafür der Agent (S. 294) auf der Maschine installiert sein muss. Solche Maschinen erscheinen im Abschnitt **Virtuelle Maschinen**. Falls ein Agent im Gastsystem installiert ist, erscheint die Maschine im Abschnitt **Maschinen mit Agenten**.

Voll-Backup

Selbstständiges Backup (S. 294), das alle Daten enthält, die für die Sicherung gewählt wurden. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.

W

Wiederauffüllbarer Pool

Ein Band-Pool, der bei Bedarf Bänder aus dem Pool **Frei Bändern** entnehmen darf.

Wiederherstellungspunkt

Tag und Zeitpunkt, zu dem die gesicherten Daten wiederhergestellt werden können.

WinPE (Windows Preinstallation Environment)

Ein minimales, funktionsreduziertes Windows-System, welches üblicherweise von OEMs und Unternehmen für Deployments, Tests, Diagnosen und Systemreparaturen verwendet wird. Eine Maschine kann in die WinPE über PXE, CD-ROM, USB-Flash-Laufwerke oder Festplatten gebootet werden. Das Acronis Plug-in für WinPE (S. 293) ermöglicht die Ausführung des Acronis Backup Agenten (S. 294) in der Preinstallation Environment.

Z

Zentrale Verwaltung

Verwaltung der Acronis Backup-Infrastruktur durch eine zentrale Verwaltungseinheit, die Acronis Backup Management Server (S. 302) genannt wird. Die zentralen Verwaltungsaktionen umfassen:

- Erstellung zentraler Backup-Pläne (S. 307) für registrierte Maschinen (S. 303) und Maschinengruppen
- Erstellung und Verwaltung statischer (S. 304) und dynamischer Gruppen (S. 299) von Maschinen (S. 302)
- Verwaltung von auf den Maschinen existierenden Tasks (S. 304)
- Erstellung und Verwaltung zentraler Depots (S. 307) zur Speicherung von Archiven

- Verwaltung von Storage Node (S. 304)
- Überwachung der Aktivitäten der Acronis Backup Komponenten, Erstellung von Berichten, Einsicht in das zentrale Log und mehr.

Zentraler Backup-Plan

Ein Backup-Plan (S. 295), der vom Management Server (S. 302) auf eine verwaltete Maschine (S. 305) verteilt wird. Ein solcher Plan kann nur durch Bearbeitung des ursprünglichen Backup-Plans auf dem Management Server modifiziert werden.

Zentraler Task

Ein Task (S. 304), der vom Management Server (S. 302) auf eine Maschine verbreitet wird. Ein solcher Task kann nur durch Bearbeitung des ursprünglichen Tasks oder zentralen Backup-Plans (S. 307) auf dem Management Server modifiziert werden.

Zentrales Depot

Ein Speicherort im Netzwerk, der vom Administrator des Management Servers (S. 302) zugeteilt wird, um als Speicherplatz für Backup-Archive (S. 295) zu dienen. Ein zentrales Depot kann von einem Storage Node (S. 304) verwaltet werden oder es ist nicht verwaltet. Die Gesamtzahl und Größe der Archive, die in einem zentralen Depot gespeichert werden können, wird nur von der Speicherplatzgröße begrenzt.

Sobald der Administrator ein zentrales Depot erstellt, werden dessen Name und der Pfad zum Depot an alle auf dem Server registrierten Maschinen (S. 303) verteilt. Die Verknüpfung zum Depot erscheint auf den Maschinen in der Liste **Depots**. Jeder Backup-Plan (S. 295), der auf den Maschinen existiert, einschließlich der lokalen Pläne, kann das zentrale Depot benutzen.

Auf einer Maschine, die nicht auf dem Management Server registriert ist, kann ein Benutzer mit entsprechenden Rechten Backups zum zentralen Depot ausführen, wenn er den vollen Pfad zum Depot verwendet. Wenn das Depot verwaltet wird, werden die Archive des Benutzers vom Storage Node ebenso wie andere Archive behandelt, die im Depot gespeichert worden sind.